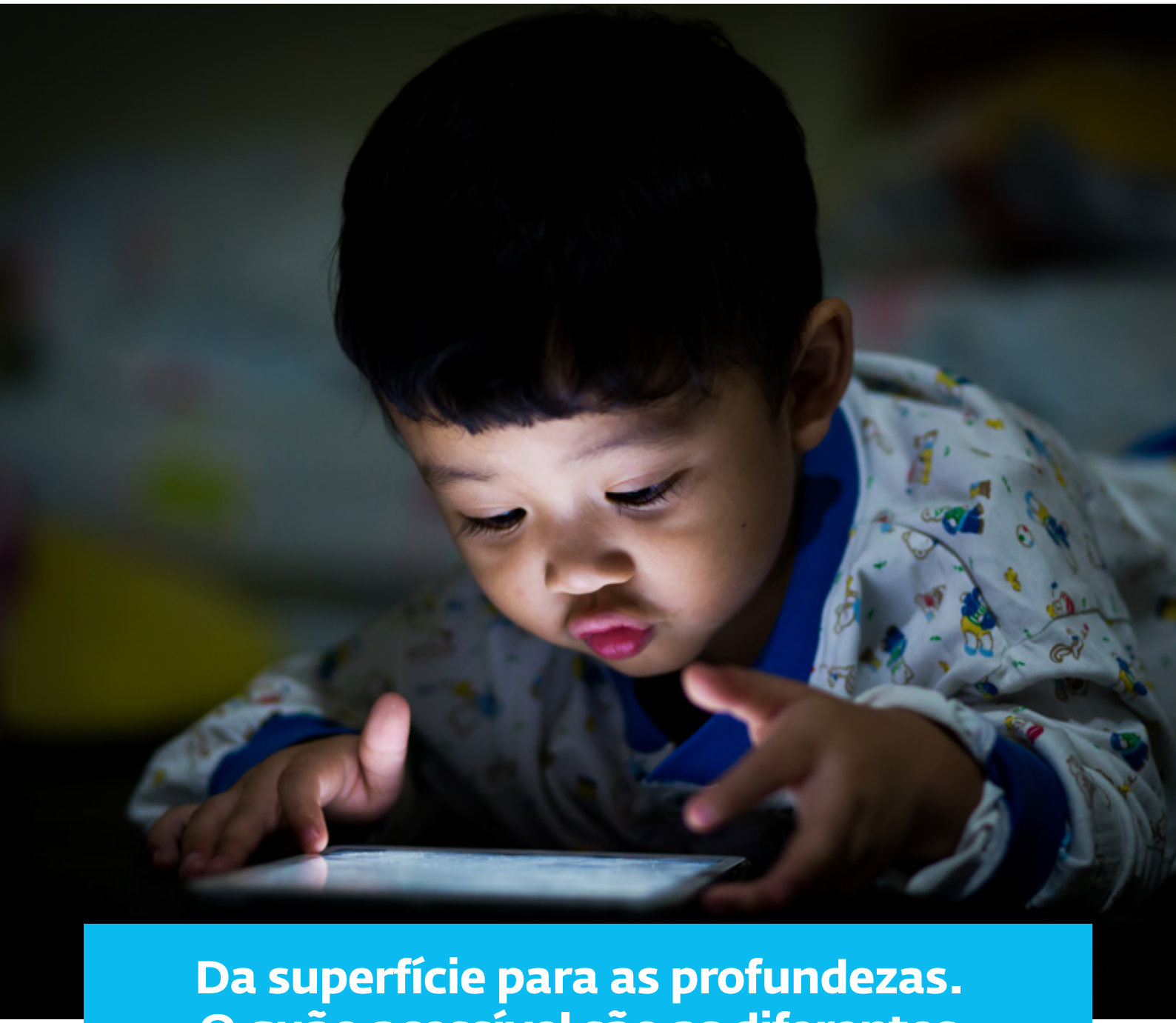
Digipais

UMA INICIATIVA DA saferkidsonline by eset



Da superfície para as profundezas. O quão acessível são as diferentes partes da internet para crianças?

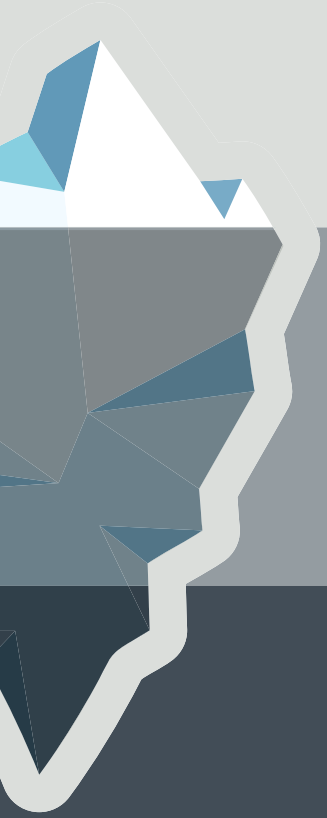
Os perigos associados com a **Dark Web** são frequentemente discutidos. Mas muitos pais ainda estão confusos sobre como esses websites realmente funcionam e quais riscos apresentam.

Descubra como se diferem a Surface Web, Deep Web e Dark Web, e como elas podem afetar seus filhos.

Por que é importante entender como funcionam as diferentes partes da internet?

Ainda que possa parecer que as piores coisas ocorrem na Dark Web, muitas interações problemáticas podem acontecer na Surface Web. Por exemplo, os predadores frequentemente não precisam de mais do que plataformas de aplicativos de chat geralmente disponíveis para se comunicar com as crianças. Por outro lado, muito do material publicado sobre as crianças nas redes sociais pode facilmente acabar em bancos de dados oferecidos na dark web.

Conhecer o relacionamento entre a **Surface**, **Deep** e **Dark Web** permite que você defina os mecanismos corretos de controle e de comunicação com seus filhos.



SURFACE WEB

A surface web consiste em websites publicamente acessíveis que os usuários podem encontrar usando mecanismos de pesquisa na internet, como o **Google**, **DuckDuckGo** ou **Bing**. Essa é a parte mais acessível da internet, onde você pode ver páginas indexadas

DEEP WEB

A parte da internet que está disponível apenas para certos grupos de pessoas, por exemplo, livros de relatório eletrônicos, conteúdo educacional voltado para uma aula específica e também as seções pagas de portais de notícias ou sistemas internos de empresas. Esses sites e conteúdos não estão acessíveis para qualquer usuário. Para procurá-los ou obter acesso, o usuário **precisa de um software especial, ferramentas ou privilégios de acesso**, porque essas páginas não estão indexadas para exibição em um mecanismo de pesquisa.

DARK WEB

Não é indexada pelos mecanismos de pesquisa e executa na dark net. Essa infraestrutura fornece anonimato para os operadores e usuários da dark web. Para se conectar à dark web, um usuário **precisa instalar software especializado como o TOR ou o serviço I2P** (Projeto de Internet Invisível).

Fonte: Manual de Segurança Digital para Professores

Enquanto uma grande parte da **Deep Web** é legal e legítima, **grandes partes da Dark Web** consistem de produtos ou conteúdo ilegal. De acordo com o *GoGuardian*, os itens encontrados na Dark Web frequentemente incluem drogas, armas não licenciadas, identidades falsas, ferramentas de hackeamento, cartões de crédito roubados, conteúdo adulto e muitos fóruns para coisas que não tem espaço na internet comum. Há também um software que torna possível pra que você acesse remotamente os computadores de outros.

No entanto, **nem tudo na Dark Web é ilegal**. Há uma grande comunidade de leitura na Dark Web e o material pode variar de ficção e livros educacionais a publicações com ideologias extremistas.

Outro serviço incomum é uma alternativa anônima ao Airbnb, **com o qual o Especialista em Consciência de Segurança da ESET, Ondrej Kubovič, deparou.** *"Ao contrário do Airbnb, este serviço não precisa de verificação de identidade, nem força os usuários a compartilhar grandes quantidades de dados. Simplesmente crie uma identidade com um apelido, sob o qual você gradualmente vai construindo uma reputação, e consiga acomodações de maneira mais independente, apenas entre outros usuários da Dark Web*", explica Kubovič.

Por que isso **pode ser atrativo** para muchas personas, incluso adolescentes, porque eles não precisam revelar tantas coisas sobre si mesmos. Por outro lado, **pode haver golpes de fuga**, onde usuários de longa data abusam de sua reputação muito boa para fazer um grande "negócio de fuga", roubar uma grande quantidade de dinheiro, excluindo sua identidade e desaparecendo logo após. **Esses são os tópicos que você pode discutir com seus filhos se eles vierem perguntar.** "Eu recomendaria explicar que os riscos são maiores na Dark Web e que há mais probabilidade de encontrar um golpista ali do que na internet comum," diz Kubovič.

Quando há o risco de uma criança ir para a Dark Web?

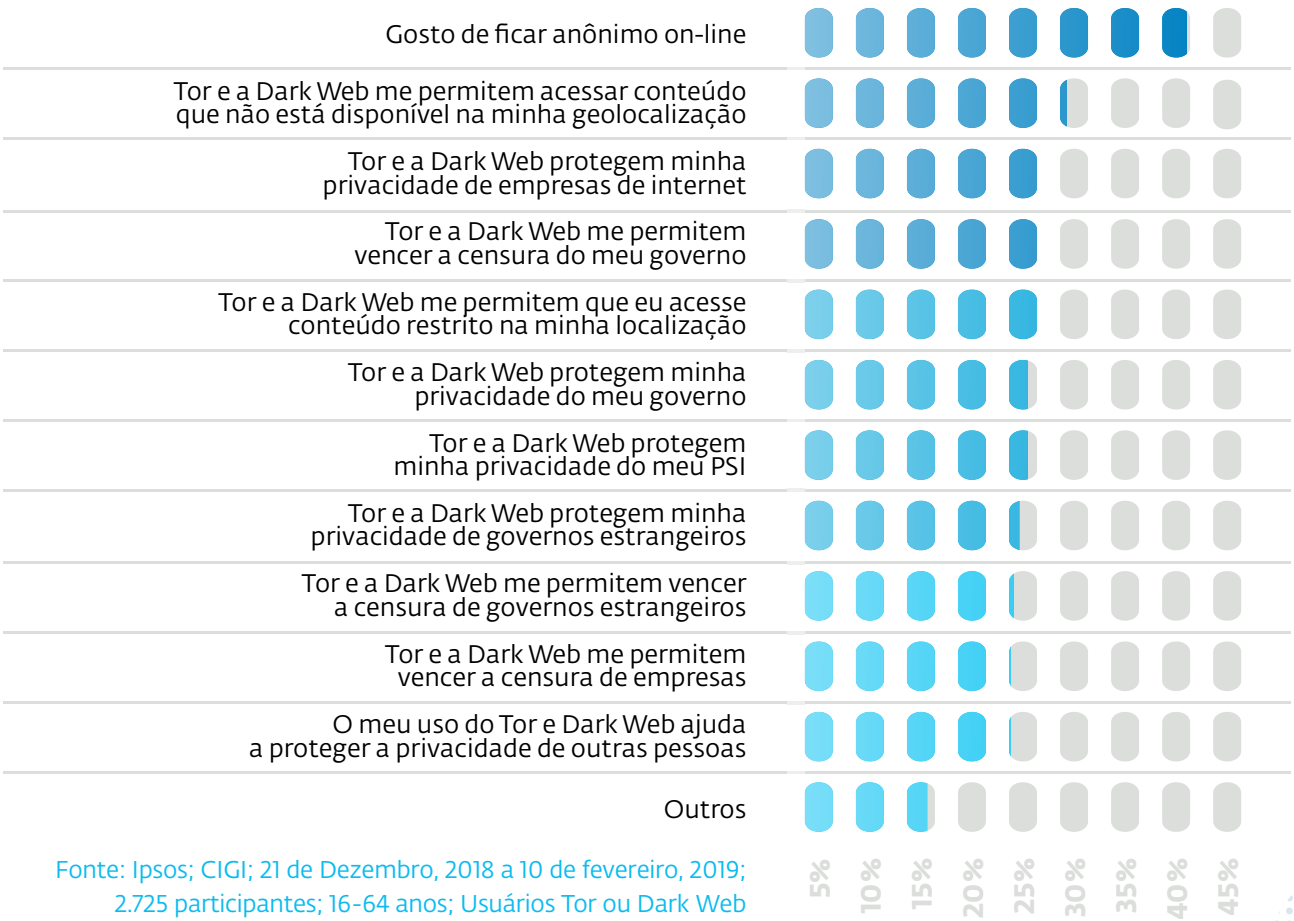
Acessar a Dark Web **requer conhecimento e técnica**. Há casos onde um estranho entra em contato com uma criança e, assim que ganha sua confiança, ele a guia através da Dark Web. No entanto, de acordo com Ondrej Kubovič, tais situações **não são muito comuns** e a maioria das crianças não sentem geralmente a necessidade de ir à Dark Web. E para as poucas que querem, isso provavelmente não vai acontecer antes da puberdade. Principalmente por conta do conhecimento técnico necessário para acessar a Dark Web, **mas também por conta do carregamento lento**.

"Se eu tivesse 14 anos de idade e meus amigos viessem e me perguntassem se quero navegar na Dark Web com eles, eu sentaria e experimentaria. Quando você é mais velho não é tão difícil, porque encontrar instruções na internet para guiá-lo através de todo o processo é fácil. ***Você não precisa se cadastrar ou criar uma conta***", explica o especialista de TI.

"Mas a I2P, e algumas vezes até a TOR, podem ser muito lentas e acho que isso ***frustraria totalmente qualquer adolescente****. As crianças de hoje não estão mais acostumadas a isso e não gostariam. Mesmo o TOR é mais lento do que um navegador comum,"* reflete Kubovič. De acordo com ele, a quantidade de conteúdo perigoso que os adolescente podem ver na Dark Web não é tão grande, mas é sempre questão da motivação, curiosidade e interesse dos indivíduos.

Motivos mais comuns para usuários acessarem a Dark Web no mundo

FEV 2019



Fonte: Ipsos; CIGI; 21 de Dezembro, 2018 a 10 de fevereiro, 2019; 2.725 participantes; 16-64 anos; Usuários Tor ou Dark Web

Quais medidas preventivas você pode tomar como pai?

Como pai, você pode fazer duas grandes coisas: Se você tem uma forte suspeita que seu(-sua) filho(a) está ativo na Dark Web, você pode verificar os sistemas operacionais software instalados em seus dispositivos. Procure pelo **TOR** (The Onion Router), **I2P**, **Freenet**; aplicativos que configuram redes virtuais privadas (**VPN**); ou uso de sistemas operacionais como **Whonix**, **Subgraph**, **Tails** ou **Qubes**. Para proteger ainda mais seus filhos, **instale um software parental e filtro de conteúdo** que possam bloquear sites.

Outro passo é pensar nas consequências e impacto de tal atividade. **Não proíba seus filhos de navegarem na Dark Web**, já que isso **apenas encoraja a curiosidade**. Se você for um pai mais tecnológico, você pode **navegar em alguns sites com seus filhos,** para mostrar a eles que não são interessantes. Tente explicar o que pode acontecer se eles visitarem a Dark Web ou quais informações sobre eles podem aparecer ali, se você ou eles compartilharem muito sobre si mesmos nas mídias sociais na Surface Web. Além disso, eles podem encontrar conteúdo perturbador, como fóruns de suicídio, casos extremos de conteúdo adulto que não está disponível na rede comum, ou podem descobrir fóruns com tópicos de negócios ilegais.

Queremos mais **Digipais** para capacitar as crianças
e ensiná-los a navegar com segurança.

Você está pronto para se juntar a nós neste desafio?

www.digipais.com.br