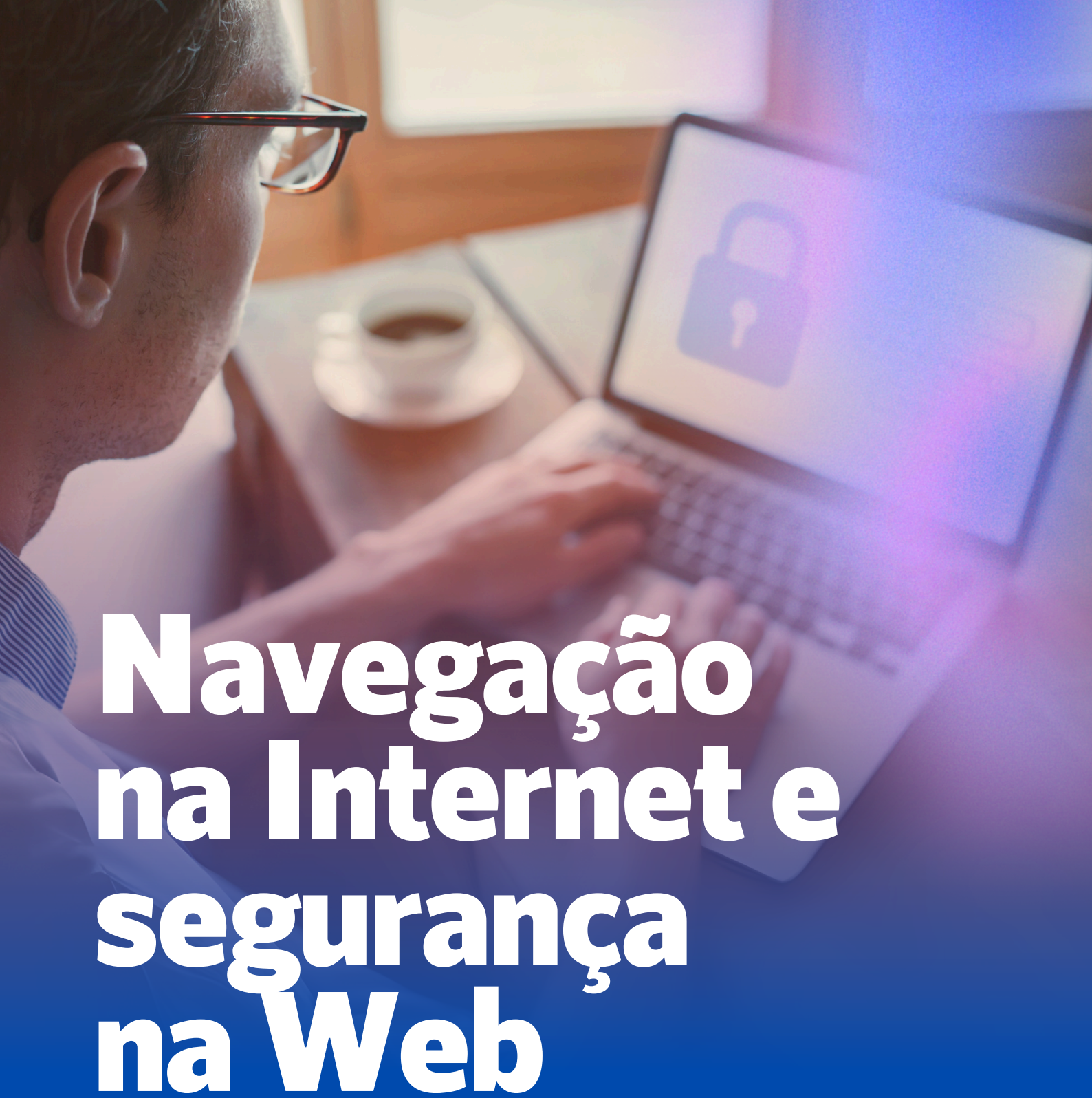


Navegação na Internet e segurança na Web

almeja

FORMAÇÃO INTEGRADA DE JOVENS E ADULTOS

Créditos

Autoria

MILTON FERREIRA DE AZARA FILHO

Mestre em Educação Profissional e Tecnológica, especialista em Segurança de Redes de Computadores, graduado em Redes de Comunicação. Servidor público federal, da Diretoria de Educação a Distância, do Instituto Federal de Goiás.

Contato: milton.filho@ifg.edu.br

Diagramação

MILTON FERREIRA DE AZARA FILHO

Revisão

ROSSELINI DINIZ BARBOSA RIBEIRO

Contato: rosselini.ribeiro@ifg.edu.br

HELEN BETANE FERREIRA PEREIRA

Contato: helen.pereira@ifg.edu.br

OLLIVER ROBSON MARIANO ROSA

Contato: olliver.rosa@ifg.edu.br



INSTITUTO FEDERAL
Goiás

Ficha catalográfica

CIP- Brasil – Catalogação na Fonte
Sistema Integrado de Bibliotecas – SIB/IFG

I59n Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Navegação na internet e segurança na web/ Instituto Federal de Educação, Ciência e Tecnologia de Goiás; Milton Ferreira de Azara Filho. – Goiânia: IFG, 2026
46 p.: il. - (Almeja: formação integrada de jovens e adultos)

ISBN 978-65-83687-22-7 (digital)

Publicação em formato pdf.

1. Segurança - web. 2. Internet – navegação segura. I. Azara Filho, Milton Ferreira de. II. Título. III. Série.

CDD 005.8

Maria Aparecida Andrade de Oliveira Tsu – Bibliotecária – CRB 1/1604

Sumário

APRESENTAÇÃO 5

HISTÓRICO E OS FUNDAMENTOS DA INTERNET 6

Alguns termos importantes 10

NAVEGAÇÃO E PESQUISAS NA WEB 13

Navegadores Web 14

Aplicativos 17

Pesquisas na Internet 18

Dicas para encontrar o que você precisa 21

BOAS PRÁTICAS PARA NAVEGAÇÃO SEGURA NA WEB 23

Segurança nas redes sociais 23

Cuidados com as compras on-line 26

Transações bancárias e pagamentos via Pix 29

Dicas gerais para navegação segura 33

DESINFORMAÇÃO E GOLPES NA WEB: SAIBA COMO SE PREVENIR 36

Desinformação 37

Golpes na Web 41

REFERÊNCIAS 45

Apresentação

ESTE MATERIAL É PARTE INTEGRANTE DO CURSO "NAVEGAÇÃO NA INTERNET E SEGURANÇA NA WEB"

Seja muito bem-vindo(a) ao e-book **Navegação na Internet e Segurança na Web**. Neste material, você será apresentado aos conceitos iniciais sobre a Internet e aos aspectos importantes para uma navegação segura.

Inicialmente, você será apresentado aos fundamentos da Internet. Para isso, faremos um percurso histórico desde a sua criação até os dias atuais.

Em seguida, você será conduzido ao imenso mar que é a Internet. Aqui, você verá como encontrar as informações de forma confiável. Essa é uma tarefa muito importante para quem está começando neste mundo.

O terceiro tópico apresentará as boas práticas para navegação segura na Internet. Aqui, você saberá como evitar golpes nas redes sociais e como realizar transações bancárias com mais segurança. Por fim, ainda neste tópico, conheceremos algumas estratégias para navegação segura na Web.

No quarto e último tópico, vamos falar sobre a desinformação na Internet. Além de aprender a não cair nas *fake news*, você saberá como se prevenir dos principais golpes aplicados na Web.

Histórico e os fundamentos da internet

O COMEÇO DA INTERNET

Você sabe o que é Internet? A todo momento estamos permeados por aplicativos, redes sociais, websites e aplicações de todos os tipos. Você sabia que YouTube, Instagram, Facebook, WhatsApp, Moodle, sites e aplicativos de banco, dentre outros, têm uma coisa em comum? Todas essas aplicações só chegam até você, seja por meio de um *smartphone* (celular) ou de um computador pessoal, por causa da Internet!

A história da internet começa no final da **década de 1950**, numa época em que os Estados Unidos e a então União Soviética competiam, ideologicamente, em um momento histórico que chamamos de Guerra Fria. Essas duas grandes potências disputavam espaço em várias áreas, como a tecnologia, a comunicação e a exploração espacial. Foi uma longa corrida para ver quem avançava mais.

Mas o que isso tem a ver com a Internet? Bom, tudo! foi nesse contexto histórico que a Internet "nasceu". Não a Internet como conhecemos hoje, claro, mas um embrião do que viria a se tornar a Rede Mundial de Computadores.

Em 1958, os EUA criaram a ARPA (Advanced Research Projects Agency) ou, numa tradução livre, Agência de Projetos e Pesquisa Avançada. Esta agência focava em pesquisas sobre comunicação e informática, principalmente. Foi então que, em 1969, a agência lançou um projeto denominado ARPANET, que visava conectar computadores em rede para fins de pesquisa e desenvolvimento. Para além das finalidades acadêmicas e científicas, este projeto visava também o desenvolvimento de uma rede em larga escala que pudesse resistir, por exemplo, a um ataque nuclear, permitindo que as informações continuassem a fluir mesmo se algumas partes da rede fossem destruídas (nic.br, 2024).

Em 1969, a ARPA criou o projeto **ARPAnet**, o primeiro embrião da Internet. Com este projeto, foi desenvolvida a primeira rede de computadores do mundo, que conectou quatro importantes universidades nos Estados Unidos.

- Universidade da Califórnia em Los Angeles (UCLA)
- Instituto de Pesquisa de Stanford
- Universidade da Califórnia em Santa Bárbara (UCSB)
- Universidade de Utah

Com o crescimento da ARPAnet, mais computadores foram sendo adicionados a rede, novas universidades e instituições foram conectadas, tornando a rede mais ampla e robusta. Por meio deste projeto, pesquisadores puderam se comunicar, compartilhar recursos e trabalhar em projetos conjuntos. Tudo isso graças à tecnologia de comutação de pacotes. A ARPAnet é muito diferente da Internet como conhecemos hoje, no entanto ela foi o primeiro grande passo para uma era de plena conectividade. A ARPAnet foi a base para o desenvolvimento da Internet moderna (nic.br, 2024; Internetsocety, 1997).

Em 1989, Tim Berners-Lee, um cientista britânico, inventou a **Word Wide Web (WWW ou Web)**. Este projeto foi inicialmente "concebido para atender à demanda por compartilhamento automatizado de informações entre cientistas em universidades e institutos ao redor do mundo (CERN, 2025)". Para isso, Berners-Lee imaginou um sistema com documentos ligados entre si, formando uma "teia" de informações (nic.br, 2024).

Com o projeto da World Wide Web, os primeiros sites vieram logo em seguida, numa era que podemos chamar de **Web 1.0**. Nesta época, os sites eram muito rudimentares, com conteúdos basicamente estáticos. Em outras palavras, as páginas web dispunham de conteúdos fixos, geralmente textos, com pouca ou nenhuma interatividade. A Web era projetada para que os usuários pudessem ler as informações, sem a possibilidade de interagir ou contribuir com o conteúdo.

Se você tem mais de 30 anos, deve se lembrar da internet discada (Dial-up). Era esse o tipo de conexão nos anos 90. A baixa velocidade na conexão também influenciava no tipo de conteúdo dos sites naquela época, já que imagens, vídeos e conteúdos mais elaborados não eram elementos apropriados para conexões desse tipo. A Web 1.0 perdurou durante toda a década de 1990 até o início dos anos 2000.

O final da década de 1990 e o início dos anos 2000 foi o período de transição para a **Web 2.0**. A evolução tecnológica e os avanços nos meios de comunicação, proporcionaram, na Web 2.0, o desenvolvimento de sites e serviços com maior interatividade. O usuário, desta vez, passou de um mero espectador para alguém que escrevia a sua própria história na Internet. A Web 2.0

> [...] é composta pelas redes sociais, pela criação instantânea de sites, pelos sites de portfólio, pelos blogs e pelos fóruns... Basicamente, por qualquer plataforma na qual você possa carregar conteúdo e torná-lo visível para outras pessoas. Além disso, ela é a web dos apps, incluindo desde serviços bancários até compras em supermercado e transporte privado. Facebook, YouTube, Wikipedia, Amazon, [...] quase todos os sites em que você faz comentários, publicações ou login são considerados parte da Web 2.0. Eles usam HTML dinâmico, e o conteúdo costuma ser disponibilizado a partir de um banco de dados (Brave, 2022).

O grande avanço da Web 2.0 foi possibilitar que os próprios usuários criassem conteúdo. As redes sociais, os blogs e os sites colaborativos são um exemplo disso. Além da melhoria nos conteúdos e na interface gráfica dos sites, a Web 2.0 proporcionou uma revolução na forma com que as pessoas interagem entre si e com os serviços na Internet. Sites de *e-commerce*, bancos digitais, redes sociais, vídeos sob demanda, aplicativos de comunicação, dentre outros, são fruto da Web 2.0.

Mas o que é um *E-commerce*?

SAIBA MAIS!

É o nome dado a um tipo de negócio que consiste na compra e venda de produtos totalmente através da internet. Materia completa publicada em **Exame.com**

Recapitulando

1958 ARPA

Em 1958, os EUA criaram a ARPA (Advanced Research Projects Agency) ou, numa tradução livre, Agência de Projetos e Pesquisa Avançada. Esta agência focava em pesquisas sobre comunicação e informática, principalmente.

1969 ARPANET

A ARPANET foi a primeira rede a implementar o protocolo TCP/IP, conectando universidades nos Estados Unidos. Desenvolvida pelo Departamento de Defesa dos EUA, foi a precursora da Internet moderna.

1989 Projeto WWW

Em 1989, Tim Berners-Lee propôs um sistema de hipermídia para compartilhar informações através de documentos interconectados, criando assim o conceito de World Wide Web (WWW).

1990s Web 1.0

Desenvolvimento de sites estáticos, pouca interação com o usuário e conteúdos basicamente para leitura. Pouca ou nenhuma imagem. Vídeos então, nem pensar!

2000s Web 2.0

Evolução da Web 1.0. Maior interatividade, surgimento dos blogs, redes sociais, início das plataformas de vídeo. O próprio usuário gerava o seu conteúdo.

2020s Dias atuais

Comunicação em tempo real, criação de comunidades globais. Redes sociais. Mudança sobre como nos comunicamos. Popularização do acesso à Internet. Internet das coisas. Inteligência artificial.

Conteúdo adaptado de **nic.br**, A história da Internet e suas tecnologias. Acesse aqui.

Alguns termos importantes

Nesse mundo da Internet existem termos e conceitos que, muitas vezes, lemos e até ouvimos, mas sequer sabemos do que se trata, não é mesmo? Agora, vamos conhecer alguns termos importantes e que serão muito úteis no seu trabalho, na escola e até mesmo no seu tempo livre!



@ (arroba)

É um sinal ou caractere convencionado para separar o nome de usuário do domínio em um endereço de e-mail. Por exemplo: anamaria1234@gmail.com. anamaria1234 é o **nome de usuário** e gmail.com é o **domínio**.



Domínio

É basicamente o endereço do site na Internet. Geralmente são nomes fáceis de lembrar. Exemplo: ifg.edu.br, gmail.com, hotmail.com, youtube.com, gov.br, google.com, dentre outros.



URL

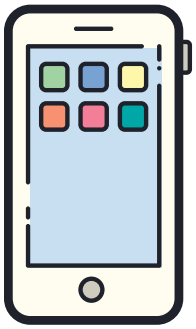
São os endereços na Internet. Incluem o domínio e outras informações. Exemplo: https://www.google.com/maps, https://mail.google.com/, https://ifg.edu.br/ead, dentre outros.

Em linhas gerais, o domínio faz parte da URL, mas ela é composta por elementos que vão além do domínio. Quer conhecer mais, **acesse aqui**.



E-mail

É uma forma de comunicação na Internet. Utilizado para troca de mensagens e documentos entre diferentes pessoas. Existem diversos serviços de e-mail, os principais são: gmail.com, hotmail.com e outlook.com.



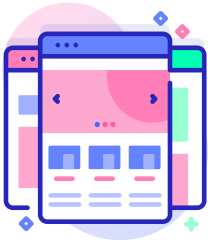
Smartphones

São uma evolução dos antigos telefones celulares. São capazes de realizar muitas das funções de um computador, como acesso à internet, envio de e-mail, acesso às redes sociais, reprodução de vídeos, dentre outros.



Google

Principal site de buscas da atualidade. É também uma empresa detentora de vários serviços, como Gmail, Google Maps, YouTube, dentre outros. Por meio do Google é possível encontrar sites e informações relevantes na Internet.



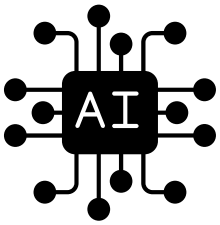
AVA ou AVEA

Ambientes Virtuais de Aprendizagem (AVA) ou Ambientes Virtuais de Ensino e Aprendizagem (AVEA) são terminologias utilizadas para se referir aos ambientes virtuais onde são oferecidos cursos on-line. O Moodle é um tipo de AVEA.



Moodle

O Moodle, acrônimo para Modular Object-Oriented Dynamic Learning Environment, uma plataforma de aprendizagem on-line que permite a criação e a gestão de cursos. É um tipo de Ambiente Virtual gratuito e amplamente utilizado ao redor do mundo.



Inteligência artificial

A inteligência artificial é um campo da ciência que se concentra na criação de computadores e máquinas que podem “raciocinar”, aprender e realizar tarefas que normalmente exigem inteligência humana (cloud.google, 2025)



Hipertexto

É um tipo de texto que não está limitado a ser linear. Hipertexto contem *links* que levam para outros textos (ou a outras páginas) (w3c, 2003).



Hipermídia

É uma extensão do hipertexto. É um tipo de hipertexto que não se limita apenas a texto. Hipermídia pode incluir gráficos, vídeos, som, imagem e outros.



Web

Web, ou www, é um espaço de informações (hipertexto e hipermídia) interconectadas e acessíveis pela Internet. A Web utiliza-se da infraestrutura da Internet para o seu funcionamento.

Navegação e pesquisas na Web

NAVEGANDO NESSE IMENSO MAR QUE É A INTERNET!

Agora que você já conhece sobre os fundamentos que constituem a Internet, vamos te apresentar algumas práticas para navegação segura. Mas antes disso, precisamos entender o significado de "**navegar na Internet**".

Navegar na Internet é o ato de acessar qualquer site ou serviço on-line. Se você acessa o YouTube, o Google, ou uma rede social, por exemplo, na prática você está navegando na Internet. Vivemos um momento em que nossos *smartphones*, computadores, tablets, smart TVs, e outros dispositivos, estão permanentemente conectados à Internet. Em outras palavras, nós estamos a todo o tempo conectados à Internet.

Pense comigo: você costuma se comunicar com os amigos e com a família pelo WhatsApp? Você tem perfil em alguma rede social? Você tem o hábito de assistir vídeos, filmes e séries on-line? Bem, se você respondeu sim a pelo menos uma dessas questões, você navega na Internet.

O ato de navegar na Internet já está incorporado nas nossas rotinas. Vivemos em um mundo conectado, com sistemas que nos dão acesso a uma gama de serviços que impactam diretamente na nossa vida *off-line*. **Aliás, o conceito de vida on-line e *off-line* já se esvaiu, é tudo a mesma coisa.**

Agendamento de exames, comida por *delivery,* corrida por aplicativo, banco on-line (internet *banking*), Pix, compras on-line, aulas on-line, provas on-line, inscrições em cursos e concursos, enfim, são uma infinidade de serviços que, embora sejam realizados virtualmente, impactam diretamente em nossa vida.

Existem duas formas básicas de acessar sites e utilizar serviços na Internet: por meio de um **navegador web** (*browser)* ou utilizando **aplicativos** em *smartphones*.

Navegadores Web

Um navegador web, ou apenas navegador, é um software que permite que os usuários naveguem e interajam com a Internet. Por meio de um navegador, você pode realizar buscas e exibir conteúdos como páginas web, imagens, vídeos, textos, entre outros tipos de dados.

Principais navegadores Web



Google Chrome

Desenvolvido pelo Google, o **Chrome** é o navegador web mais usado no mundo, atingindo quase 70% dos usuários.
Dica: Tente acessar as ferramentas e serviços do Google com o **Chrome**, por serem do mesmo fabricante, sua experiência na navegação será melhor!



Mozilla Firefox

Desenvolvido pela Mozilla Foundation, o **Firefox** é um navegador bastante utilizado. Embora tenha perdido espaço para o **Chrome**, continua sendo uma ótima opção para navegação.



Microsoft Edge

Desenvolvido pela Microsoft, o **Edge** é o mais novo dos três navegadores. É uma evolução do antigo Internet Explorer e foi lançado pela Microsoft no ano de 2015. É também uma boa opção para navegação.
Dica: Tente acessar as ferramentas e serviços da Microsoft com o **Edge**!



Safari

O **Safari** é o navegador web padrão no **iPhone** e sistemas operacionais macOS. Ele possui uma integração com outros dispositivos Apple, sincronizando favoritos, histórico e outras informações do usuário.
Dica: Se você tem um **Iphone**, certamente você utiliza o **Safari** como navegador!

REALIZE UMA PESQUISA NO GOOGLE, BAIXE ESTES NAVEGADORES E FAÇA UM TESTE!

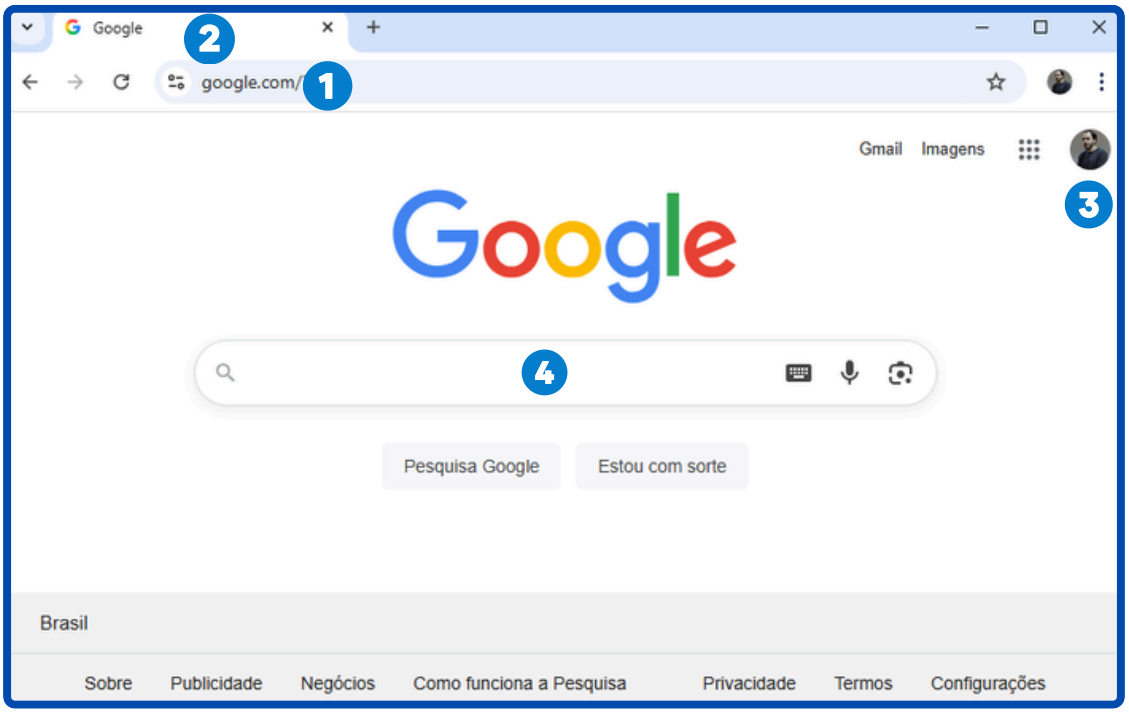
Como posso acessar o navegador no meu computador ou *smartphone*?

DICA!

No **computador**, os navegadores ficam disponíveis, na maioria dos casos, na **área de trabalho**. Você pode encontrá-los também na barra de tarefas ou no menu iniciar.

No ***smartphone* (celular)**, o ícone do navegador fica disponível na tela inicial ou nas telas adjacentes. Você pode rolar a tela para o lado até encontrar o ícone do navegador.

Agora que você já conhece os principais navegadores e sabe como acessá-los, em um computador ou *smartphone*, vamos entender como é o visual e a estrutura de um navegador. Para isso, utilizaremos como base o Google Chrome, principal navegador da atualidade.



1 **Barra de endereços:** é o espaço onde você deve digitar o endereço do site. Ex: google.com, ifg.edu.br, ead.ifg.edu.br, dentre outros.

2 **Abas do navegador:** em uma só janela é possível abrir quantas forem necessárias. Cada aba representa o acesso a um site diferente. Mas, atenção! Quanto maior a quantidade de abas abertas, maior é o consumo de memória no computador, o que pode deixá-lo mais lento!

3 **Perfil do usuário autenticado no navegador:** isso permite que informações de navegação sejam importadas em computadores diferentes. Se você está começando, vá com calma! Esta não é uma funcionalidade necessária nesse momento.

4 **Campo de busca:** como o site acessado neste exemplo é o Google, o mais famoso buscador da atualidade, este é o espaço onde será digitado o termo que se queira buscar na Internet.

Aplicativos

Conhecidos também como "*apps*", os aplicativos são *softwares* projetados para serem utilizados em dispositivos móveis, como *smartphones* ou *tablets*. Por meio dos aplicativos, você pode ter acesso a serviços específicos, como plataformas de vídeos, redes sociais, *delivery* de comida, compras on-line, transporte por aplicativo, entre outros.

Diferentemente dos navegadores, os aplicativos são projetados para prover acesso a funcionalidades e serviços específicos. Em outras palavras, se em um navegador você "escolhe" o site ou o serviço que você vai acessar, por meio de um aplicativo você terá acesso a funcionalidades e serviços específicos daquele aplicativo.


YouTube


Instagram



Uber


Facebook


WhatsApp

Se você tem um *smartphone* com acesso à Internet, é possível que você já tenha utilizado a maior parte desses aplicativos. Cada um deles apresenta uma função distinta:

- YouTube: vídeos
- Instagram: rede social
- Uber: transporte
- Facebook: rede social
- WhatsApp: comunicação

Os aplicativos são normalmente adquiridos através de lojas de aplicativos, como a **App Store (Apple)** e o **Google Play Store (Android)**.

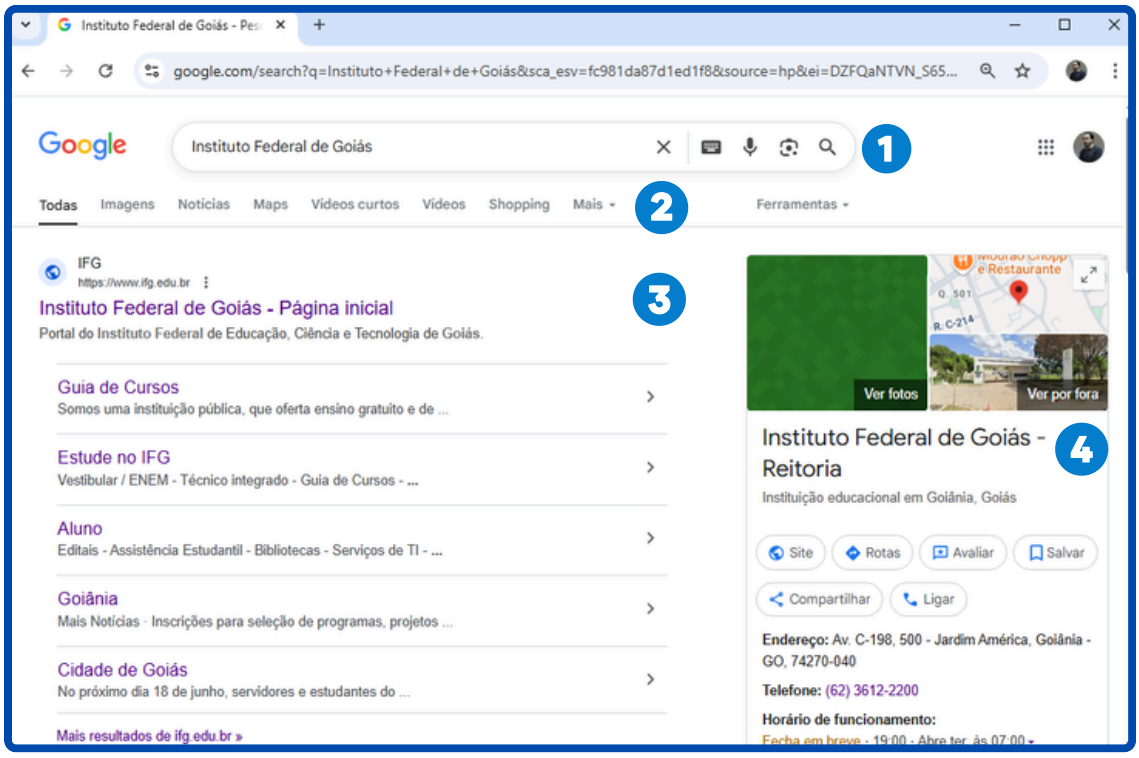
Pesquisas na Internet

Os sites de buscas são provavelmente os serviços mais acessados na Internet. Saber como pesquisar um termo, uma frase, um site, ou mesmo um tipo de serviço, é uma tarefa importante para quem está começando. Além de saber como fazer as pesquisas, é preciso entender como os resultados aparecem para você e em que nível esses resultados são confiáveis. Você sabia, por exemplo, que não é porque uma informação "está" no Google, que ela é verídica? Mas para entender o porquê disso, precisamos nos aventurar e compreender como o Google funciona!

O Google é um mecanismo de busca automatizado que utiliza "softwares conhecidos como rastreadores da Web, que exploram a Web regularmente para encontrar páginas a serem adicionadas ao [...] índice (developers.google, 2025)". Nesse sentido, a primeira premissa que precisa ser desconstruída é de que o conteúdo, o site ou o serviço "está no Google". Na verdade, o Google apresenta como resultado as informações relevantes para a sua consulta, mas o conteúdo em si não está no Google, ele está disponível no site de origem.

Quando você pesquisa um termo no Google, o buscador pesquisa o índice de páginas correspondentes e retorna os resultados mais relevantes para a sua consulta. **Então quer dizer que se duas pessoas fizerem a mesma consulta, o resultado pode ser diferente? Sim, isso mesmo!** A relevância de um resultado que aparece quando você busca por algum termo, depende de centenas de fatores, que podem incluir informações como a sua localização, o seu idioma, o dispositivo que você está utilizando no momento (computador, tablet, *smartphone*), entre muitos outros fatores (developers.google, 2025).

Diferentes tipos de pesquisas resultam em formatos de resultados diferentes. Por exemplo: se você pesquisa por "**Instituto Federal de Goiás**" **(IFG)**, que é uma instituição pública de ensino, o resultado mostrará, provavelmente, o site oficial e, talvez, as primeiras páginas que estão sob a forma de *links* referenciados na página principal. Como o IFG tem sedes físicas (seus câmpus e reitoria), a pesquisa tende a mostrar como resultado a localização da sede mais próxima a você.



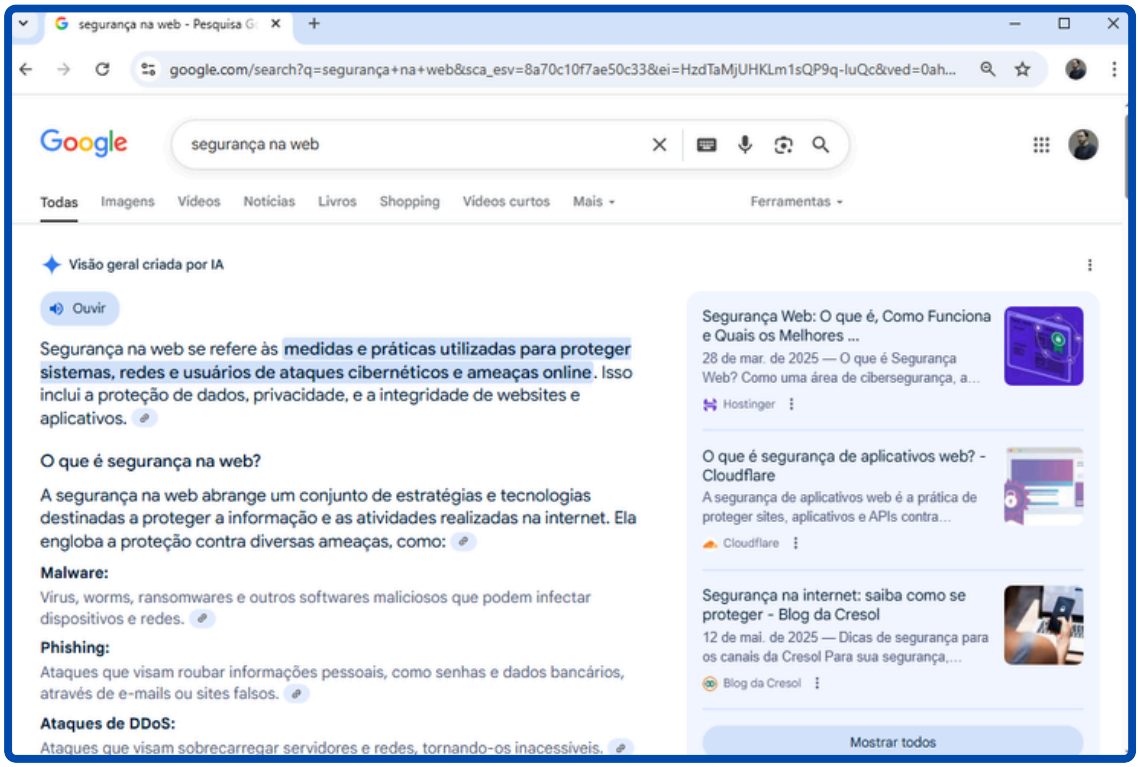
1 **Campo de busca:** espaço pelo qual você entrará com o termo, frase, site ou serviço que você deseja encontrar. Além de texto, você pode realizar a pesquisa por voz ou imagem.

2 **Tipos de pesquisa:** o primeiro menu apresenta todos os resultados da pesquisa. Mas você pode filtrar os resultados por imagens, notícias, localização (maps), videos, entre outros. Ao clicar em "ferramentas", você pode filtrar os resultados por idioma ou data de publicação, por exemplo.

3 **Resultado da pesquisa:** o conteúdo depende do tipo de pesquisa realizada pelo usuário. O formato do conteúdo pode variar entre *links* para os principais sites, textos gerados por inteligência artificial, notícias recentes, entre outros.

4 **Localização:** se a pesquisa for sobre um termo que se referir a instituições ou serviços que tenham sede física, o resultado tende a retornar o lugar mais próximo à sua localização.

Por outro lado, se o objeto da pesquisa for um **termo abstrato** ou **algum conceito**, o resultado tentará trazer a definição ou as informações que a inteligência artificial do Google entende como mais relevantes.



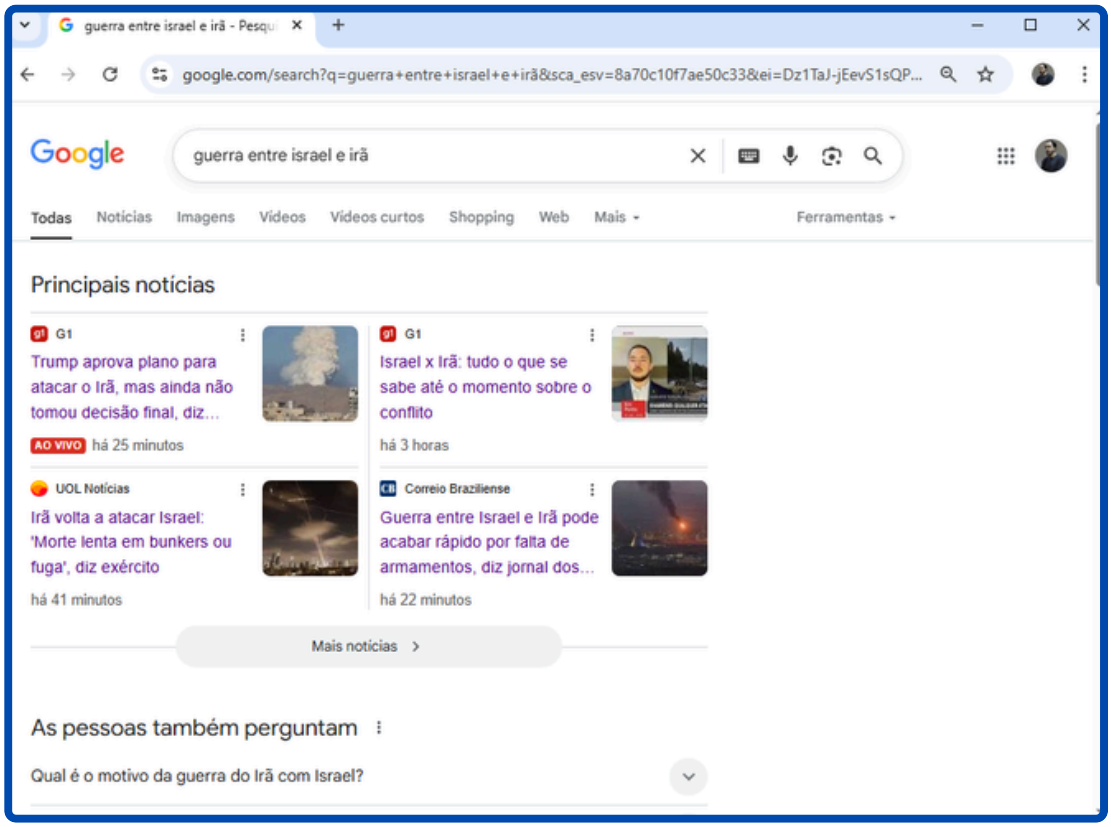
Se você rolar a página, *links* para outros sites começam a aparecer. Em geral, na seguinte ordem:

1. *Links* patrocinados, ou seja, sites ou serviços que contratam do Google uma forma de impulsionar os seus dados ou serviços.
2. *Links* para sites ou serviços que o Google entende como mais relevantes para a sua pesquisa.

A inteligência artificial está sempre correta? **ATENÇÃO!**

Nem sempre! A **inteligência artificial generativa** é um modelo computacional treinado a partir de dados e textos disponíveis na Internet. Podemos dizer, portanto, que a **IA** "aprende" com base em textos e dados que já existem e que estão espalhados pela Web. E se parte desses dados forem incorretos? A depender da situação, a IA pode gerar informações **falsas, imprecisas ou mesmo inventadas**. **Tome cuidado!**

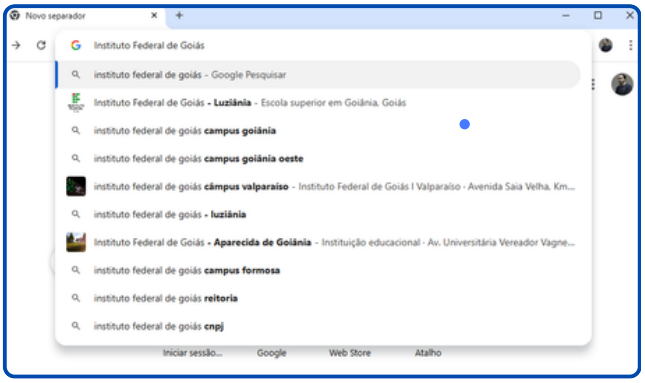
É importante que você saiba que existem dezenas, senão centenas de fatores que influenciam nos resultados de uma busca no Google. Se você estiver pesquisando, por exemplo, por um fato recente ou uma notícia atual, o Google tende a mostrar como resultado as publicações mais atuais e que ele entende como relevantes. A pesquisa abaixo foi realizada em 18 de junho de 2025, às 19h30.



Dicas para encontrar o que você precisa

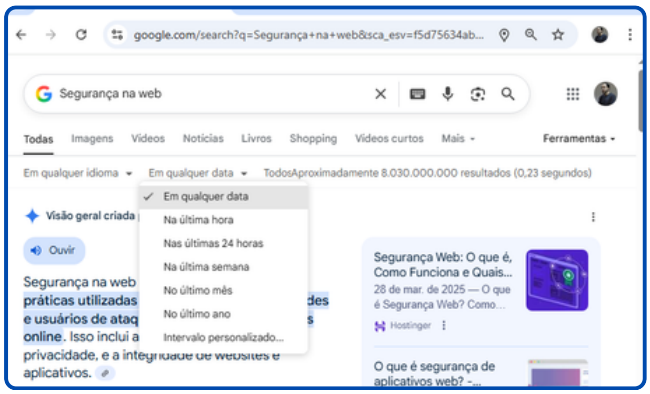
1 Pesquise direto na barra de endereços do navegador

Se o Google for o mecanismo de busca padrão do seu navegador, você pode fazer a busca direto na barra de endereços do navegador.



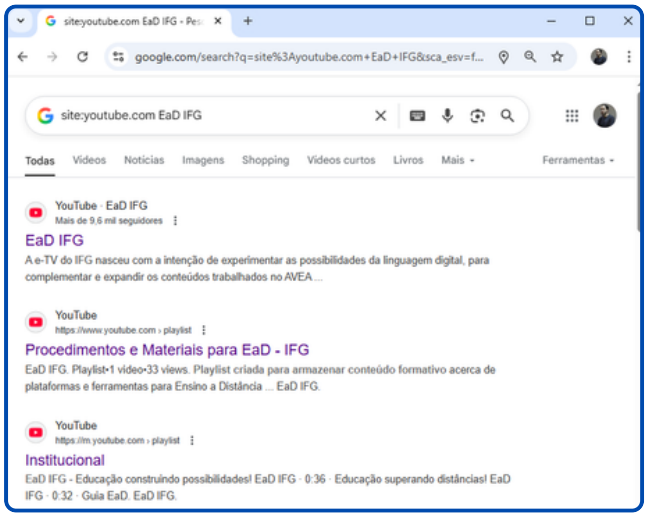
2 Filtre os resultados

Você pode filtrar o resultado da busca por idioma, data de publicação, entre outros. Para isso, clique em “Ferramentas” e selecione o filtro desejado. Diferentes termos de busca possibilitam diferentes formatos de filtro. Faça o teste!



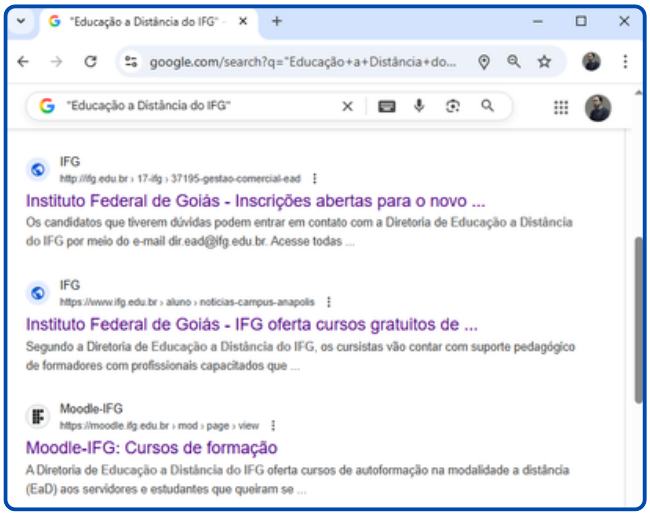
3 Pesquisa sm sites específicos

Vamos supor que você quer pesquisar no Google sobre **EaD IFG**, mas quer resultados obtidos diretamente do YouTube. Digite no campo de pesquisa: **site:youtube.com EaD IFG**. Este tipo de busca pode ser feito em qualquer site ou mesmo em páginas específicas dentro do site.



4 Resultados de correspondência exata

Coloque o termo ou a frase que você quer consultar entre aspas duplas. O resultado vai te apresentar as páginas e os trechos que contém exatamente o que foi buscado. Por exemplo: “Educação a Distância do IFG”. Um bom teste é pesquisar pelo seu nome completo no Google, entre aspas duplas. Por exemplo: “José Antônio da Silva Santos”. Faça o teste!



Conteúdo adaptado de **Backlinko**. 21 dicas de pesquisa do Google para encontrar exatamente o que você deseja. **Acesse aqui.**

Boas práticas para navegação segura na Web

NA DÚVIDA, NÃO CLIQUE!

Acesso a compras on-line, pagamentos via Pix, transações pelo aplicativo do banco, comunicação em tempo real, redes sociais interativas, enfim, são muitas as facilidades proporcionadas pela Internet. No mundo real, no entanto, junto a essas facilidades, vêm os riscos. Sim, e são muitos os riscos que você pode correr por não se atentar aos aspectos de segurança na Web.

Em um primeiro momento, vamos entender como lidar com as redes sociais e com a avalanche de informações geradas por elas.

Segurança nas Redes Sociais

Se você tem perfil em alguma rede social, provavelmente já se deparou com discussões, xingamentos, *bullyng* ou mesmo alguma situação de exposição desnecessária. Nesse sentido, é importante refletirmos sobre o papel das redes sociais e sobre como a interação com estas pode ser nociva, dependendo de como nos comportamos.

A privacidade nas redes sociais é um assunto que deve ser levado a sério. Entenda: a "exposição excessiva e a coleta abusiva de dados podem dar a outros a capacidade de influenciar e limitar suas escolhas, além de facilitar a ação de pessoas mal-intencionadas (cert.br, 2023, p. 2)."

A seguir, algumas dicas para a navegação segura nas redes sociais:

1

Pense muito bem antes de postar!
Nas redes sociais as informações são propagadas sem o nosso controle. Uma vez postado, sempre postado. Por mais que o seu perfil seja fechado, entenda que você está em um local público. Tudo o que você posta agora, poderá ser visto por alguém no futuro.

2

Proteja o acesso à sua conta
O acesso à sua conta na rede social pode ser valiosa para golpistas. Eles podem se aproveitar da confiança entre você e seus contatos para aplicar golpes. Para evitar que isso aconteça, crie senhas fortes e ative a verificação em duas etapas. Nunca acesse redes sociais de computadores públicos!

3

Não acredite em tudo que você vê na rede social
As redes sociais estão inundadas por informações falsas. Acreditar em qualquer informação que você vê na sua *timeline* facilita a ação de golpistas. Busque sempre informações em outras fontes e tenha cuidado ao clicar e compartilhar *links*.

4

Cuidado com o que você curte e compartilha
O ato de curtir e compartilhar um post ou um *link* transmite para a rede social que você gostou daquele conteúdo. Se esse conteúdo for indevido, isso pode gerar consequências, inclusive judiciais. Atente-se aos seus hábitos na redes sociais, eles podem dizer muito sobre você.

5

Configure o que outros usuários podem postar sobre você
Existem configurações que podem limitar a marcação ou a menção sobre você em postagens. Tente sempre configurar para que as marcações e as menções sejam previamente analisadas por você antes de serem publicadas em seu perfil.

6

Cuidado com aplicativos de terceiros
Aplicativos de terceiros, como jogos, testes, edição de fotos, podem capturar suas informações pessoais e até o seu histórico de navegação para fins abusivos. Pense muito bem antes de dar acesso a aplicativos de terceiros.

7

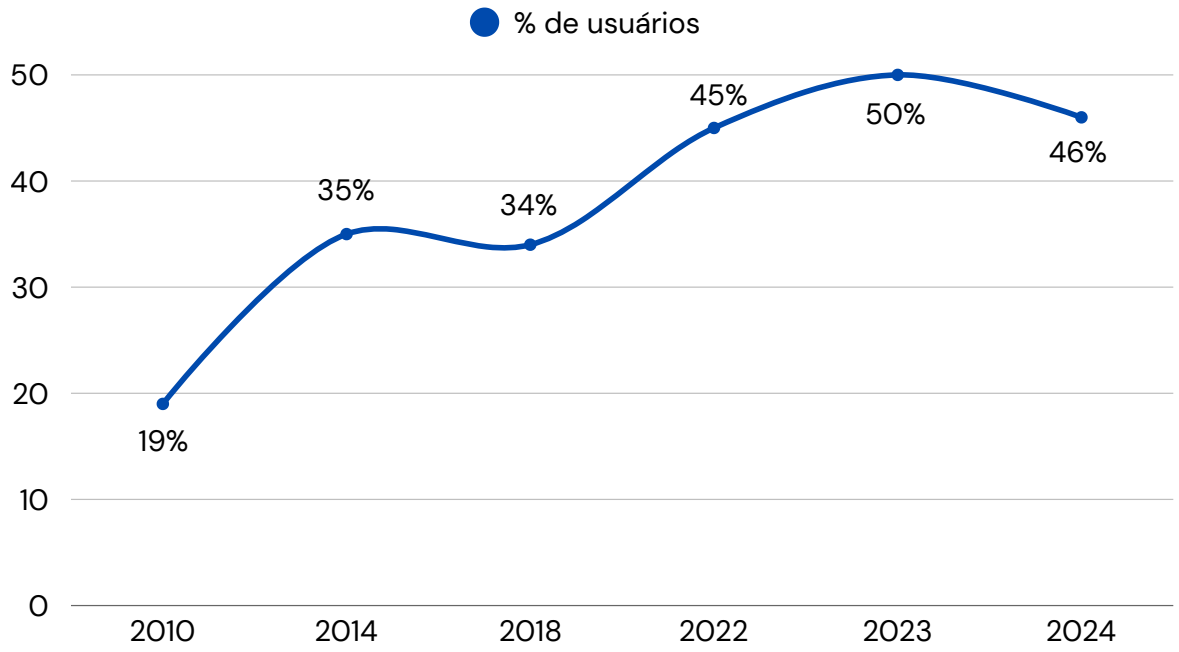
Mantenha a intimidade off-line
Lembre-se, fotos e vídeos íntimos podem ser usados para constranger ou chantagear pessoas. Evite compartilhar imagens e vídeos de situações íntimas.

Conteúdo adaptado de **Cert.br**. Redes Sociais. **Acesse aqui.**

Cuidados com as compras on-line

Realizar compras pela internet tornou-se uma tarefa trivial no nosso dia a dia. Sites de compras, os chamados *e-commerce*, são cada vez mais comuns. O que antes fazíamos presencialmente, indo até a loja física, hoje podemos fazer pela Internet. As grandes empresas de varejo, além de manter as suas lojas físicas, disponibilizam também sites para vendas on-line.

A pesquisa TIC Domicílios aponta para o aumento na proporção de usuários que compraram produtos e serviços pela Internet entre 2010 e 2024:



% de usuários que compraram produtos e serviços pela internet entre 2010 e 2024

TIC Domicílios

Em 2024, 46% dos usuários de Internet (**73 milhões de pessoas**) compraram produtos e serviços pela Internet. Com tantas pessoas realizando compras pela Internet, a incidência de golpes também aumentou. Mais do que nunca você precisa se atentar aos aspectos de segurança para realizar as suas compras pela Internet. Vejamos algumas dicas:

1

Vai comprar pela Internet? Utilize um dispositivo seguro.
Sabe aquele *smartphone* antigo e com o sistema operacional desatualizado? Evite realizar compras a partir desses dispositivos. Sistemas ou aplicativos desatualizados podem ser uma porta de entrada de vírus que visam furtar os seus dados e praticar fraudes. Se for comprar pelo computador, certifique-se de que seu antivirus e que o sistema operacional estejam atualizados. Evite realizar compras pelo *smartphone* ou computador de outra pessoa.

2

Se estiver comprando pelo computador, verifique minunciosamente o endereço do site.
Criminosos podem clonar um site e te induzir a acessá-lo. Algumas vezes, a diferença no endereço eletrônico pode ser sutil, mas o bastante para te levar para outro site, por exemplo: amazo**N**.com e amazo**M**.com. Evite clicar em *links* que direcionem aos sites de compras.

3

Confirme se o site possui um certificado de segurança.
O certificado de segurança ajuda a comprovar a identidade de um site. Esse tipo de certificado mantém a segurança dos dados que você envia para o servidor, ou seja, dados bancários, senhas, informações pessoais, entre outras. Mas como identificar se o site possui um certificado de segurança? Verifique na barra de navegação se há a imagem de um cadeado fechado. Caso exista, o site possui um certificado. Opa! Sinal verde!

4

Verifique se você está interagindo com o perfil oficial da empresa.
Ao contatar empresas de comércio eletrônico via redes sociais, certifique-se de que o perfil é legítimo. Redes sociais são uma boa alternativa para contato com as empresas, mas antes veja se o perfil provém de uma conta comercial verificada. Se possível, confira se o perfil na rede social é o mesmo que está descrito no site da empresa.

5

Desconfie de valores muito abaixo do mercado.
Quando o produto ou o serviço estiver muito abaixo dos oferecidos em outros sites, desconfie! Golpistas utilizam esta prática para atrair e fisgar sua vítimas. Sempre que for comprar alguma coisa na Internet, pesquise em muitos sites, veja a opinião de outras pessoas que já compraram e confira os requisitos básicos de segurança. Cautela nunca é demais!

6

Atenção aos *links* de ofertas recebidos por SMS ou e-mail!
Se você receber ofertas por e-mail, SMS, aplicativos de mensagens ou mesmo em redes sociais, tenha muita atenção ao clicar. Existem golpistas que se aproveitam do nome de lojas famosas para praticarem crimes. Priorize sempre as compras realizadas diretamente pelo site ou pelo aplicativo da loja.

Conteúdo adaptado de **Internet Segura** e **Comércio via Internet**. Conteúdos formativos distribuídos pelo cert.br, nic.br e cgi.br.

Transações bancárias e pagamentos via Pix

Realizar transações financeiras pela Internet tem se tornado mais fácil e rápido. Os bancos digitais, aos poucos, estão substituindo as agências físicas. Pare e pense: quantas agências bancárias você já viu fechar as portas? Isso quer dizer que os bancos estão indo à falência? Muito pelo contrário! **Significa que os serviços digitais estão substituindo as agências físicas**. Nesse sentido, é importante que você saiba como utilizar o aplicativo do banco com segurança.

Os aplicativos de banco devem ser baixados exclusivamente em lojas oficiais, como a **App Store (Apple)** e o **Google Play Store (Android)**. Lembre-se! Tenha cuidado ao baixar aplicativos, principalmente os aplicativos de banco! Caso o acesso à conta bancária seja pelo navegador, certifique-se de que você está acessando o site oficial do banco. Confira a URL e verifique se a conexão com o site é segura (https).

Manter o *smartphone* atualizado é uma prática importante, ainda mais quando você utiliza este dispositivo para realizar transações financeiras. Segundo a Febraban (Federação Brasileira dos Bancos), entidade que representa os principais bancos brasileiros, as transações bancárias pelo celular (*smartphone*) cresceram 251% nos últimos 5 anos e representam hoje 7 a cada 10 transações financeiras (Febraban, 2024). À medida que aumentam as transações, aumentam também os riscos. Veja como se prevenir:

1 **Sempre ative uma senha no seu celular. Habilite a biometria, caso possível!**
O acesso ao seu celular deve ser protegido por biometria (se houver esta funcionalidade), caso contrário habilite uma senha de acesso de maior complexidade. Essa é a primeira barreira para evitar problemas com transações bancárias pelo celular.

2 **Habilite o bloqueio automático de tela.**
Se seu aparelho for furtado, roubado ou mesmo esquecido em algum local, o bloqueio automático de tela poderá evitar que outra pessoa tenha acesso aos seus aplicativos.

3 **Conheça os canais oficiais do seu banco.**
Se você estiver utilizando o computador para fazer transações bancárias, certifique-se de que o site do banco é o correto. Confira o endereço eletrônico e evite acessar o site do banco por meio de *links* de terceiros.

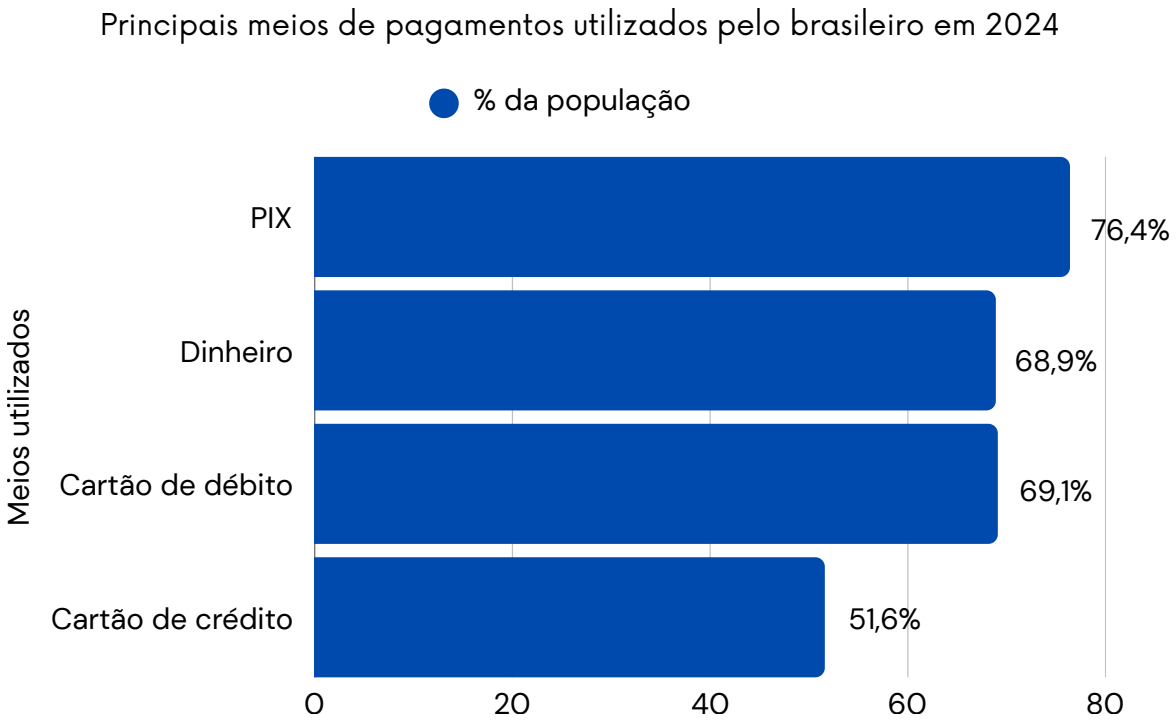
4 **Não grave as senhas do seu banco no celular.**
Senhas no bloco de notas ou anotadas em outros aplicativos podem ser facilmente encontradas por golpistas. Se outra pessoa tiver acesso ao seu celular desbloqueado, poderá ter acesso às senhas. Não tire fotos de senhas.

5 **Não compartilhe senhas com terceiros.**
Por maior confiança que tenha em alguém, não compartilhe suas senhas. As senhas de acesso aos seus aplicativos devem ser pessoais e intransferíveis. A senha de acesso ao banco, então, é mais sensível ainda.

6 **Ajuste os limites para transações financeiras.**
Adequar os limites das operações pode te ajudar a reduzir possíveis prejuízos em casos de fraudes. Analise as suas finanças e tente reduzir os limites de transferências entre contas e Pix. Avalie também os limites de crédito para evitar futuros problemas. Utilize somente o necessário.

De acordo com a pesquisa TIC Domicílios (2024), 84% dos usuários de Internet que compraram produtos ou serviços pela Internet utilizaram o Pix como forma de pagamento. Em outras palavras, quase 140 milhões de brasileiros e brasileiras utilizaram o Pix como meio de pagamento em compras on-line.

Para além das compras on-line, o Pix se tornou a principal forma de transação financeira, ultrapassando o dinheiro vivo, cartão de débito e cartão de crédito. A pesquisa realizada pelo Banco Central do Brasil, intitulada "O brasileiro e sua relação com o dinheiro", realizada em 2024, aponta que 76,4% da população utilizou o Pix para realizar compras e/ou pagamentos.



Fonte: Banco Central do Brasil (2024). Colocar o link no Branco Central do Brasil.

Com a crescente popularização do Pix como meio de pagamento, cresce também a insegurança. Mas saiba que existem formas de tornar as suas transações mais seguras, vamos ver algumas?

1

Não clique em *links* enviados por SMS ou WhatsApp!
Os bancos não enviam *links* para cadastro ou efetivação de transações via SMS ou WhatsApp. A chave Pix é cadastrada diretamente no aplicativo do banco e todas as transações também acontecem por lá. Se você receber alguma propaganda para baixar o aplicativo do Pix, é golpe!

2

Sempre confira os dados do destinatário antes de efetivar o Pix.
Se você vai realizar uma transação via Pix, seja um pagamento, transferência entre contas, entre outras, verifique os dados do destinatário antes de finalizar a transação. Se estiver pagando um boleto via Pix, confira atentamente os dados do destinatário, pois existem golpes que simulam boletos e que podem te induzir a realizar pagamentos para criminosos.

3

Desconfie de solicitações de dinheiro pelo WhatsApp. Sabe aquele seu parente ou amigo que um belo dia aparece no WhatsApp, dizendo que aconteceu alguma coisa com ele e pedindo um Pix de determinado valor? Pois é, pode ser golpe! Se for alguém conhecido, faça uma ligação ou chamada de vídeo para confirmar.

4

Evite realizar transações bancárias em redes Wi-Fi públicas. A segurança nessas redes não é adequada para esse tipo de transação. Evite fazer login no aplicativo do seu banco nesse tipo de rede. Se for fazer um Pix, utilize o pacote de dados móveis ou aguarde até chegar em um local que tenha acesso a uma rede segura.

Acesse mais dicas de segurança sobre o Pix

SAIBA MAIS!

O Banco Central do Brasil explica como se prevenir de golpes envolvendo Pix. **Acesse o vídeo**. Se preferir, use o Código QR ao lado!

Conheça o Mecanismo Especial de Devolução do Pix (MED)

SAIBA MAIS!

O Banco Central do Brasil explica como bloquear e até recuperar pagamentos fraudulentos envolvendo Pix. **Acesse o vídeo**. Se preferir, use o Código QR ao lado!

Dicas gerais para navegação segura



Navegação segura (https)

Verifique sempre se o site que você está acessando estabelece este tipo de comunicação segura. Veja se o site apresenta o famoso "cadeadinho fechado" na barra de navegação. Esse cadeado é uma forma visual, escolhida pelos navegadores, de indicar que o site acessado utiliza a comunicação segura com o protocolo HTTPS. Se você tem dúvida sobre como identificar o cadeado, **clique aqui** e assista ao vídeo. Se preferir, aponte a câmera do seu celular para o QR-Code ao lado!



Senhas seguras

Seja muito cuidadoso ao elaborar senhas, principalmente quando se trata de sites de compra, transações bancárias e redes sociais. Evite utilizar partes do seu nome ou datas de nascimento de familiares. Uma senha ideal é aquela que é fácil de ser lembrada, mas difícil de ser descoberta por outras pessoas ou por programas de computador. Tente definir senhas com diferentes caracteres (letras, números e caracteres especiais). Se precisar, anote a senha antes, mas lembre-se, mantenha sempre a anotação em local seguro!



Atenção ao clicar em *links*

Seja cuidadoso ao clicar em *links*, independente de como foram recebidos ou de quem os enviou. Desconfie de *links* enviados por pessoas desconhecidas. Leia atentamente a mensagem e se parecer um golpe, não clique!

Os bancos não te enviam *links*. Sites e serviços do governo também não te enviarão *links*. Moral da história: se você desconfia da mensagem ou do *link* recebido, não clique!



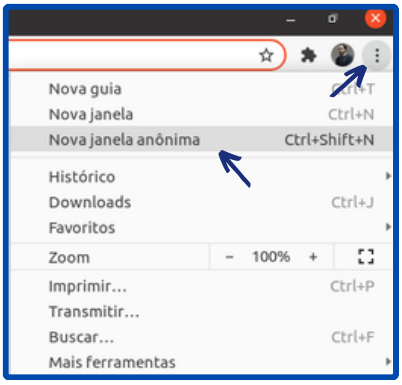
Modo de navegação anônima

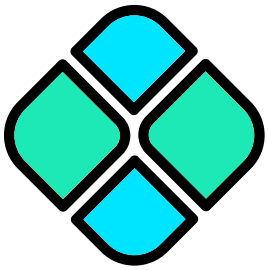
Uma forma de manter a segurança durante a navegação em dispositivos compartilhados é usar o navegador em modo anônimo, pois neste modo as páginas visitadas não serão armazenadas no histórico e os dados de navegação serão excluídos quando o navegador for fechado.

Este modo de navegação é ideal, por exemplo, nos computadores do laboratório de informática, caso você esqueça sites abertos e autenticados.

No Google Chrome, por exemplo, para ativar o modo de navegação anônima, basta digitar no teclado, quando o navegador estiver aberto, o comando **Ctrl+Shift+N**.

Outra forma é clicar nos três pontos verticais na barra superior direita. Depois, clique em nova janela anônima. Vale lembrar que mesmo navegando em modo anônimo, o usuário não fica invisível. Ou seja, a navegação anônima não oculta sua navegação do seu empregador, provedor de acesso à internet, nem dos sites que você visita!





Dicas de uso do Pix

Lançado em 2020 pelo Banco Central do Brasil, o Pix é um sistema de pagamento instantâneo e completamente digital. Ao realizar pagamentos via Pix, sempre confira os dados do destinatário. Nome completo, CPF ou CNPJ são dados que você deve conferir antes de efetivar o pagamento. Lembre-se, todo cuidado é pouco! Seu celular também é sua carteira!



Se a esmola é demais, desconfie!

Sabe aquele aparelho celular que você tanto quer comprar? Um belo dia você recebe um anúncio pela metade do preço. **Desconfie!** Sites de compra e venda na Internet podem ser bons locais para a realização desse tipo de negócio, mas antes verifique a reputação do vendedor. Veja se ele costuma entregar o que vende, por exemplo. Busque sempre a opinião de outras pessoas que também compraram deste vendedor. Quando fizer compras em sites on-line (*e-commerce*), acesse o site https://reclameaqui.com.br e pesquise sobre a reputação da empresa.



Autenticação em dois fatores

A maioria dos aplicativos e sites oferecem a funcionalidade de autenticação em dois fatores. Conhecida também como **verificação em duas etapas**, este método adiciona uma camada extra de proteção ao login de contas ou dispositivos. Essa autenticação consiste na adição de um segundo fator à senha usual. Por exemplo, código por SMS, dados biométricos, códigos por e-mail, entre outros.

Desinformação e golpes na Web: saiba como se prevenir

NEM TUDO O QUE PARECE, É!

A Web é uma extensão da nossa vida “real”. Na verdade, hoje, a vida “real” se misturou com a vida “virtual”. As nossas interações sociais, seja no mundo real seja no virtual, moldam o nosso comportamento e a forma com que enxergamos o mundo. Educação, respeito e cordialidade, são características que devemos levar também para as interações na Web.

Além de buscar sermos sempre cordiais na Web, precisamos ter bom senso e inteligência para diferenciar informações falsas e tendenciosas que circulam nas redes. Os boatos, as *fake news*, os conteúdos manipulados, as imagens e os vídeos falsos são formas de desinformação e causam muitos danos para a sociedade.

Evite compartilhar notícias e informações que você não tem certeza da veracidade. Se você usar o bom senso, vai perceber que na maioria dos casos a notícia, o post na rede social ou a imagem que circula no grupo de WhatsApp da família **é tão sem sentido**, que basta refletir um pouco para identificá-la como falsa. Antes de compartilhar, respire, pense um pouco e avalie se aquela informação é de fato verdadeira. Não faça nada no impulso!

Desinformação

A desinformação é um termo utilizado para se referir a conteúdos ou práticas que contribuam para a disseminação de **informações falsas**, **imprecisas** ou mesmo **tendenciosas**, e que podem ser utilizadas para manipular pessoas e afastá-las da realidade (tre.go, 2023; internetsegura, 2020). Na velocidade em que os conteúdos são divulgados na Web, precisamos ter muito cuidado com o que compartilhamos.

Antes de conhecermos alguns tipos de desinformação, precisamos entender a diferença entre um **fato** e uma **opinião**. Saber diferenciar uma opinião de um fato é o primeiro passo para não ser enganado por notícias e informações falsas.

Fato	Opinião
Um fato é algo que pode ser comprovado. Fatos são **objetivos** e podem ser comprovados por meio de observação, evidências, dados ou fontes confiáveis.	É uma forma de ver ou interpretar um fato ou situação. A opinião é **subjetiva**, ou seja, reflete sentimentos, crenças ou valores pessoais.

Você pode ter uma opinião ou mesmo uma interpretação sobre um fato, mas isso não muda o fato. **Fato é fato**, não vai mudar de acordo com a sua opinião. A charge a seguir ilustra bem isso:



Charge de Marcos S. Souza
Fonte: Blog do IFSC (2023).

Note que o quadrado não deixa de ser um quadrado, mesmo que um outro observador tenha a opinião de que é uma bola. Aliás, essa afirmação nem chega a ser uma opinião, porque o quadrado é comprovadamente um tipo de quadrilátero, ou seja, um polígono de quatro lados. Uma bola não tem quatro lados, portanto um quadrado não é uma bola. O observador poderia dizer que a cor amarela do quadrado é bonita, que o quadrado poderia ser um pouco maior, ou que aquele quadrado está em um local inapropriado, por exemplo. Essas sim são opiniões válidas, porque derivam do **fato** de que aquele objeto é um quadrado.

Vamos a mais um exemplo: sabe quando alguém diz algo do tipo "**pra mim, a Terra é plana, tenho certeza!**". Essa afirmação até parece uma opinião, mas na verdade não é. A forma da Terra é comprovada por cientistas, astronautas e até pelas fotos tiradas do espaço. A terra não é plana, quadrada ou mesmo um disco só porque alguém acha que ela é. A realidade concreta, a ciência e as evidências provam que a terra é **esférica**. Então, dizer que que a Terra tem outra forma não é uma opinião válida, **é só uma afirmação errada mesmo**.

Quer saber por quê a Terra é esférica?

SAIBA MAIS!

Daniel Nunes, do canal Tem Ciência, explica como descobrimos que a Terra é uma esfera. **Acesse o vídeo**. Se preferir, use o Código QR ao lado!

Agora que já sabemos diferenciar um fato de uma opinião, vamos conhecer as principais formas de desinformação.

Conteúdo manipulado

Sabe aquela situação em que você recebe uma imagem no WhatsApp, que até parece real, mas que tem alguma coisa estranha? Pois então, o conteúdo pode ter sido manipulado intencionalmente para causar desinformação! Com a inteligência artificial em alta, é perfeitamente possível que fotos sejam deliberadamente alteradas e, ainda assim, pareçam reais.

Esse tipo de desinformação ocorre quando um conteúdo ou alguma informação verdadeira é manipulado intencionalmente com o objetivo de enganar. Inclui a manipulação de textos, notícias, imagens e até vídeos.

Informação fora de contexto

Acontece quando um conteúdo verdadeiro tem o seu contexto distorcido com a intenção de enganar. Fotos, imagens, vídeos e notícias, por mais que sejam de fato verídicas, podem ser publicados em contextos, ou seja, em momentos anteriores ao fato ocorrido. Geralmente são imagens, vídeos ou conteúdos antigos, publicados como se fossem atuais para justificar alguma informação enganosa.

Conteúdo fabricado

Pode ser disseminado por meio de texto, imagens ou até vídeos. Via de regra, é um tipo de conteúdo que não tem nenhuma ligação com a realidade, criado exclusivamente com o objetivo de enganar. Imagens geradas por inteligência artificial, sites com conteúdos falsos, posts com informações fabricadas, são exemplos desse tipo de conteúdo.

Diante de tanta desinformação, o que podemos fazer para identificar conteúdos manipulados, fabricados ou tirados de contexto? Se você recebeu alguma imagem, um *link* ou uma notícia pelo WhatsApp ou por outro meio, confira alguns passos para identificar se o conteúdo é verdadeiro ou não.

1

A fonte da imagem, do *link* ou da notícia é conhecida?
Esse conteúdo veio de onde? Foi feito por qual veículo de comunicação? Qual site? Foi checado por alguma agência de notícias? Desconfie sempre que um conteúdo for compartilhado sem a fonte ou com a fonte desconhecida. Evite compartilhar conteúdos que você não tenha certeza da fonte.

2

O título do conteúdo é excessivamente chamativo?
Desconfie! Matérias jornalisticas e conteúdos checados e validados não costumam ter títulos chamativos ou sensacionalistas. Os títulos muito chamativos são uma estratégia para chamar a atenção de pessoas desapercebidas e causar desinformação.

3

A data da notícia ou do post é recente?
Uma das primeiras coisas que você precisa analisar é a data em que o conteúdo foi publicado. Pode ser que ele esteja sendo utilizado deliberadamente fora de contexto. Lembre-se, não é porque uma informação é verídica, que ela se torna verdadeira no contexto atual.

4

Preste atenção na qualidade do texto.
Uma das características dos textos produzidos por veículos de comunicação profissionais, é a clareza na escrita. Se o texto tem erros de ortografia, frases muito apelativas e títulos absurdos ou sensacionalistas, desconfie!

5

Por fim, seja crítico!
A Internet possibilitou que milhões de pessoas pudessem expressar as suas opiniões sobre quaisquer assuntos. É como se todo mundo entendesse de tudo, e não é assim que as coisas funcionam. Já vimos que a opinião é diferente de um fato. Seja crítico, inclusive, em relação aos conteúdos que você acompanha na mídia profissional. É importante conhecer e explorar canais de comunicação diversos.

Conteúdo adaptado de **IFSC** e **Unesco**

Quer conhecer mais a fundo como enfrentar a desinformação?

SAIBA MAIS!

Conheça o Guia prático para enfrentar a desinformação, disponibilizado pela Unicef. **Acesse o Guia**. Se preferir, use o Código QR ao lado!

Golpes na Web

Com tantos sites e serviços na Web, golpistas estão sempre criando novas formas para enganar e tirar vantagem das pessoas. Já vimos que a Internet é uma "mão na roda" quando se trata do acesso aos mais diferentes serviços, desde compras, transações bancárias e até o cadastro em programas sociais. Mas junto a essas comodidades, vem as preocupações.

Aposto que você já recebeu mensagens de texto no seu celular informando sobre uma compra que foi feita no seu cartão, ou que uma transferência bancária foi realizada, sem você nem ter conta neste banco. Pois é, são golpistas tentando te fazer ligar para centrais de atendimento falsas ou te induzir a clicar em *links* maliciosos.

Existem centenas, senão milhares, de outros tipos de golpes na Web. Desde os mais classicos, como o do exemplo anterior, até os golpes "do momento", que se aproveitam das novidades tecnológicas mais atuais. A seguir, vamos citar alguns tipos de golpes e como evitá-los.



Golpe do presente

Do nada você recebe uma oferta de um produto, seja por e-mail, mensagem de texto ou até mesmo pelo WhatsApp. Pode ser um presente, um brinde, ou até um dinheiro que está "perdido" no INSS. O golpista, então, pede alguns dados pessoais ou a foto do seu rosto (selfie), alegando que a informação serve para finalizar a entrega ou confirmar um cadastro. De posse desses dados, o golpista poderá abrir uma conta ou até contratar um empréstimo em seu nome por meio do reconhecimento facial. **Veja mais** sobre esse golpe no site do Banco Central do Brasil.



Golpe da falsa central de atendimento

Os mais variados tipos de abordagens. Na ligação, os golpistas costumam causar um impacto emocional e senso de urgência, alegando tentativas de invasão na conta, compras suspeitas ou atualizações de segurança no aplicativo.

O falso funcionário é cordial, fala bem, com educação e utiliza recursos tecnológicos para simular uma central de atendimento real. Resultado: o golpista pode solicitar que você realize operações na conta, seja pelo aplicativo do celular ou mesmo pelo caixa eletrônico. É aí que acontece o golpe! O falso atendente te induz a fornecer dados sensíveis, como a senha do cartão ou do aplicativo do banco, por exemplo.

Nunca forneça a senha de acesso ao aplicativo do banco!

ATENÇÃO!

O banco nunca irá entrar em contato com você para te pedir dados pessoais e senhas de acesso. Se alguém ligar para o seu telefone e pedir que você confirme dados sensíveis, desligue imediatamente a chamada! Quer saber mais sobre esse tipo de golpe, **clique aqui** ou acesse o Código QR ao lado.



Golpe do WhatsApp

Nesse tipo de golpe os criminosos tentam clonar a conta de WhatsApp da vítima em outro aparelho. Para obter o código de segurança enviado por mensagem de texto, o criminoso envia uma mensagem se fazendo passar por algum tipo de serviço de atendimento ao cliente, como a validação de uma compra, uma promoção imperdível ou um prêmio que você ganhou. É aí que o golpista consegue clonar o seu número de WhatsApp em outro aparelho e se fazer passar por você.



Golpe do número novo

Quem nunca recebeu uma mensagem no WhatsApp do tipo: "mãe, troquei meu número de telefone. Anota aí". Para tornar o golpe ainda mais persuasivo, os criminosos colocam a foto da pessoa no perfil do WhatsApp. Depois de uma conversa curta, o golpista inventa uma situação urgente, dizendo que foi roubado ou que precisa pagar uma conta atrasada, por exemplo. É aí que entra o pedido de transferência bancária, pix ou até o pagamento de um boleto falso. Esse tipo de golpe geralmente acontece com pessoas idosas ou com pouca intimidade com os recursos tecnológicos.

Como se prevenir desse tipo de golpe? É recomendado ocultar a foto do perfil para pessoas que não estão na sua lista de contatos. Isso pode evitar que criminosos usem a sua foto para aplicar golpes. Se alguém entrar em contato com você dizendo que o número de telefone mudou, entre em contato com o número anterior, seja por mensagem ou por chamada de vídeo, para confirmar se realmente o número mudou. Antes de realizar qualquer ação, certifique-se de que aquela pessoa é quem de fato diz ser. Nunca aja por impulso.



Golpe do boleto falso

Costumamos pagar muitas contas por meio de boletos. IPVA, condomínio, aluguel, inscrições em concursos ou processos seletivos, enfim, são muitos os serviços que podem ser pagos via boleto bancário. Mas você sabia que criminosos podem criar boletos falsos e te induzir a realizar pagamentos indevidos? Pois é, isso acontece muito e você precisa ficar atento para não cair em golpes desse tipo.

Como se prevenir desse tipo de golpe? Antes de pagar o boleto, verifique se o nome do beneficiário do pagamento é uma pessoa física ou a empresa contratada. Verifique também se o banco destinatário é o mesmo que consta no boleto. Desconfie de códigos de barras com falhas e evite imprimir boletos fora do site ou do e-mail oficial do serviço que você contratou. Atente-se à URL do site que você está contratando o serviço. A conexão é segura? O site é idôneo? Fique atento e confira os dados do boleto antes de realizar o pagamento.

5 dicas para não cair no golpe do boleto falso

SAIBA MAIS!

O Banco Central do Brasil te explica como não cair no golpe do boleto falso. **Clique aqui e acesse o vídeo**. Se preferir, use o Código QR ao lado!

Golpe do falso Pix

Envolve o envio de um comprovante de transferência falso para enganar a vítima, que acredita ter recebido um valor e, por engano, devolve o dinheiro para o golpista ou realiza alguma ação baseada nessa informação falsa. Os golpistas podem usar comprovantes falsos ou criar situações de urgência para induzir a vítima ao erro. Caso você receba alguma mensagem desse tipo, verifique primeiro o seu extrato bancário. Caso exista de fato um depósito feito na sua conta, utilize a funcionalidade de devolução do Pix porque o dinheiro retornará à mesma conta do pagador. Não aceite sugestões do suposto pagador para devolver o dinheiro numa conta diferente da que fez o depósito. Quer saber mais sobre o bolpe do falso Pix, **acesse a página do Banco Central do Brasil**.

Referências

BLACKLINKO. **21 Google Search Tips to Find Exactly What You Want**. Disponível em: https://backlinko.com/google-search-tips. Acesso em: 30. jun. 2025.

BRAVE. **Web3: Qual a diferença entre web 1.0, 2.0 e 3.0?**. Disponível em: https://brave.com/pt-br/web3/versus-web1-and-web2/. Acesso em: 22 jun. 2025.

CERN. **The birth of the Web**. Disponível em: https://home.web.cern.ch/science/computing/birth-web. Acesso em: 21 jun. 2025.

CETIC.BR. **TIC Domicílios**. Disponível em: https://cetic.br/pt/pesquisa/domicilios/. Acesso em: 20. jul. 2025.

CLOUD.GOOGLE. **O que é inteligência artificial (IA)?**. Disponível em: https://cloud.google.com/learn/what-is-artificial-intelligence?hl=pt-BR. Acesso em: 22 jun. 2025.

DEVELOPERS.GOOGLE. **Guia detalhado sobre como a Pesquisa Google funciona**. Disponível em: https://developers.google.com/search/docs/fundamentals/how-search-works?hl=pt-br. Acesso em: 30. jun. 2025.

FEBRABAN. **Transações bancárias pelo celular crescem 251% em cinco anos e hoje representam 7 a cada 10 do total**. Disponível em: https://portal.febraban.org.br/noticia/4146/pt-br/. Acesso em: 20. jul. 2025.

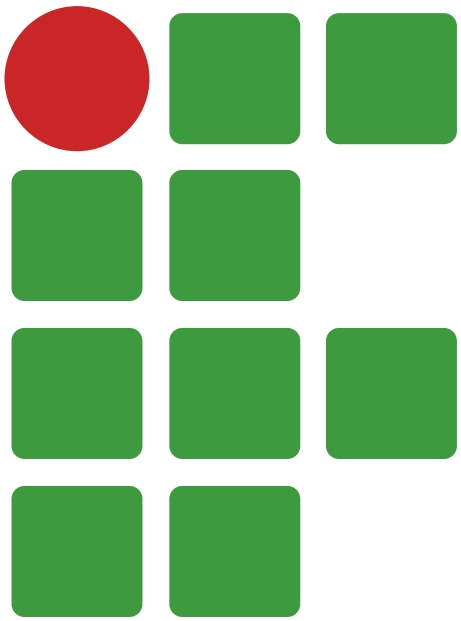
INTERNETSEGURA. **Quero Saber**. Disponível em: https://www.internetsegura.pt/FakeNews. Acesso em: 01. ago. 2025.

INTERNETSOCIETY. **A Brief History of the Internet**. Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/. Acesso em: 20 jun. 2025.

NIC.BR. **A história da Internet e suas tecnologias** - da Guerra Fria a 2024. Disponível em: https://nic.br/noticia/na-midia/a-historia-da-internet-e-suas-tecnologias-da-guerra-fria-a-2024/. Acesso em: 20 jun. 2025.

TRE.GO. **Fake news x desinformação**: entenda qual é a diferença entre os termos. Disponível em: https://www.tre-go.jus.br/comunicacao/noticias/2023/Agosto/fake-news-x-desinformacao-entenda-qual-e-a-diferenca-entre-os-termos. Acesso em: 25. jul. 2025.

W3C. **What is HyperText**. Disponível em: https://www.w3.org/WhatIs.html. Acesso em: 30. jun. 2025.



INSTITUTO FEDERAL

Goiás



Conhecer os conceitos e os fundamentos da Internet é o primeiro passo para uma navegação segura. Vivemos permanentemente conectados a aplicativos, redes sociais, websites e aplicações de todos os tipos. Isto, por si só, já acende um alerta para a forma com que interagimos com essas plataformas em rede. Acesso à compras on-line, pagamentos via Pix, transações por aplicativos bancários, comunicação em tempo real, redes sociais interativas, enfim, são muitas as facilidades proporcionadas pela Internet. No mundo real, no entanto, junto a essas facilidades, vêm os riscos. A Web é uma extensão da nossa vida "real". Na verdade, hoje, a vida "real" se misturou com a vida "virtual". As nossas interações sociais, seja no mundo real ou no virtual, moldam o nosso comportamento e a forma com que enxergamos o mundo. Educação, respeito e cordialidade, são características que devemos levar também para as interações na Web.