

GUIA RÁPIDO:

INTERNET E SEGURANÇA DIGITAL NA AMAZÔNIA

Inclusão digital para a gestão de comuns e
proteção territorial na bacia do Tapajós



FICHA CATALOGRÁFICA

COMO CITAR

Guia rápido [recurso eletrônico]: internet e segurança digital na Amazônia : inclusão digital para a gestão de comuns e proteção territorial na bacia do Tapajós / coordenação geral Fernanda Carreira e Antonio José Mota Bentes ; coordenação da pesquisa Kena Chaves e Eric Macedo ; pesquisa e elaboração Eric Macedo, Maria Letícia de Alvarenga Carvalho e Samela Bonfim. - São Paulo : FGVces ; Santarém, PA : Sapopema, 2025.

36p. – (Projeto inclusão digital para a gestão de comuns e proteção territorial na bacia do Tapajós - Indica Tapajós)

Inclui bibliografia.

ISBN: 978-85-94017-36-9

1. Grupos sociais - Amazônia. 2. Inclusão digital. 3. Internet. 4. Internet - Medidas de segurança. I. Carreira, Fernanda. II. Bentes, Antonio José Mota. III. Chaves, Kena. IV. Macedo, Eric. V. Carvalho, Maria Letícia de Alvarenga. VI. Bonfim, Samela. VII. Fundação Getulio Vargas.

CDU 004.056(811.3)

Ficha catalográfica elaborada por: Cristiane de Oliveira CRB SP-008061/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

COMUNICADO

Este material foi elaborado pela Fundação Getulio Vargas e pela Sociedade para a Pesquisa e Proteção do Meio Ambiente, com apoio da União Europeia e da Fundação Charles Stewart Mott, para contribuir com o debate público sobre conectividade e monitoramento territorial independente. Não objetiva influenciar legislação específica ou campanha política.





EXPEDIENTE

Realização

Centro de Estudos em Sustentabilidade da Fundação Getulio Vargas (FGVces) e Sociedade para a Pesquisa e Proteção do Meio Ambiente (SAPOPEMA)

Coordenação Geral

Fernanda Carreira (FGVces) e Antonio José Mota Bentes (SAPOPEMA)

Coordenação da pesquisa

Kena Chaves e Eric Macedo

Pesquisa e elaboração

Eric Macedo, Maria Letícia de Alvarenga Carvalho e Samela Bonfim

Conceituação e revisão técnica

Antonio José Mota Bentes, Kena Chaves, Tainá Holanda e Wandicleia Lopes

Projeto Gráfico

Mandalla Comunicação & Design

Direção de arte

Sâmila Braga

Criação de projeto gráfico e diagramação

Thalia Silva e Mateus Emanuel

Projeto

Inclusão digital para a gestão de comuns e proteção territorial na bacia do Tapajós (INDICA TAPAJÓS)

Apoio

União Europeia e Mott Foundation



SUMÁRIO

06 APRESENTAÇÃO

07 Quem somos

08 Conectando...

20 Como usar a Internet de forma saudável?

21 A juventude conectada

22 Conteúdo Inadequado

23 Conteúdo ilícito

23 Cyberbullying

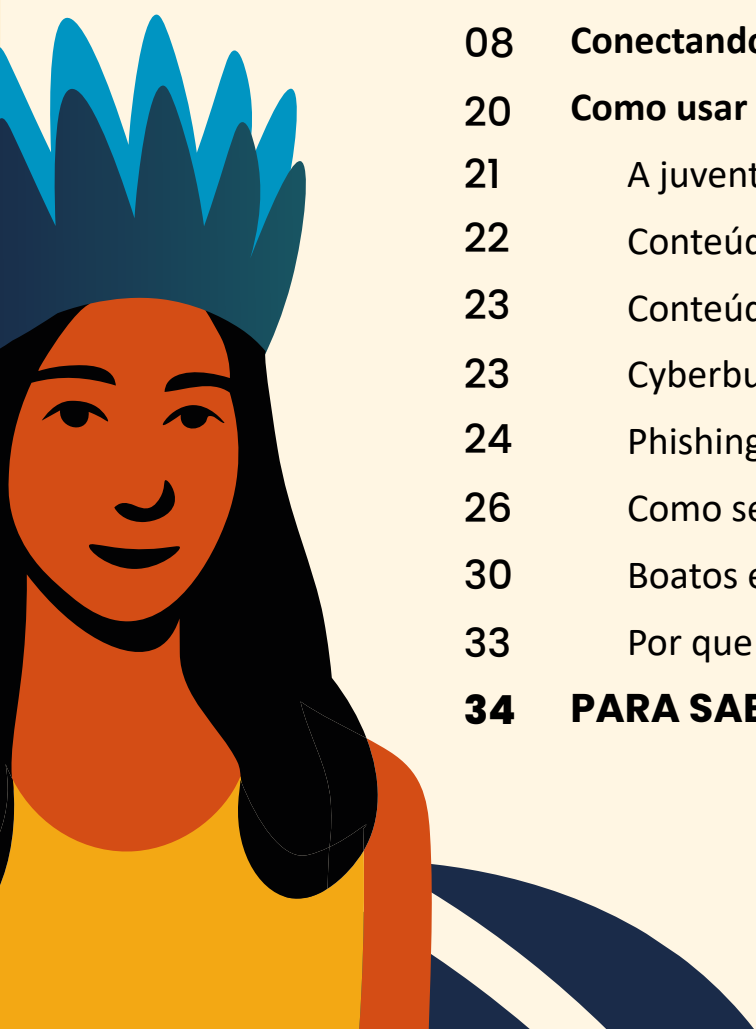
24 Phishing e golpes online

26 Como se proteger dos perigos da Internet?

30 Boatos e notícias falsas

33 Por que esses cuidados são importantes?

34 PARA SABER MAIS



APRESENTAÇÃO

A Internet tem chegado cada vez mais depressa aos territórios dos povos e comunidades tradicionais da Amazônia. Seja para se comunicar com parentes e amigos, para permitir atendimentos de saúde à distância, dar uma força nos estudos, ou acessar serviços públicos, as novas tecnologias vêm ganhando centralidade para diferentes modos de vida. Nesse contexto, surge também um novo desafio: como utilizar a Internet de forma segura, aproveitando o que ela tem de melhor a oferecer.

Formulado no âmbito do projeto *Inclusão Digital para Gestão de Comuns e Proteção Territorial na Bacia do Tapajós – INDICA TAPAJÓS*, este guia foi escrito com o objetivo de ajudar comunidades na Amazônia a se orientar neste novo ambiente que é a Internet e a se proteger contra alguns dos problemas encontrados com mais frequência no mundo digital.

A publicação está dividida em dois capítulos. O primeiro traz um glossário com os principais termos e conceitos

relacionados à Internet, além de alguns exercícios práticos para facilitar o acesso a ferramentas e serviços importantes disponíveis na rede. O segundo traz alertas e cuidados para navegar na Internet de forma segura, protegendo-se de conteúdo inadequado, golpes, jogos de azar e notícias falsas, entre outros perigos.

Esperamos que o guia sirva como material de consulta para comunidades e como suporte a oficinas de capacitação, oferecendo um ponto de partida para fortalecer a autonomia digital das comunidades da Amazônia. Ao unir os conhecimentos tradicionais à tecnologia usada com sabedoria, é possível transformar a Internet em uma aliada na defesa do território, na valorização da cultura e no fortalecimento de redes de apoio. Com preparo e atenção, cada conexão pode abrir caminhos para novas oportunidades, mantendo viva a proteção dos territórios e modos de vida.

Boa leitura!

QUEM SOMOS

O Projeto Indica Tapajós

Executado pelo Centro de Estudos em Sustentabilidade da Fundação Getúlio Vargas (FGVces) em parceria com a Sociedade para a Pesquisa e Proteção do Meio Ambiente (SAPOPEMA), o projeto Inclusão Digital para a Gestão de Comuns e Proteção Territorial na Bacia do Tapajós (Indica Tapajós) tem o objetivo de fortalecer estratégias de monitoramento territorial independente (MTI) na Amazônia por meio do acesso à conectividade e ferramentas digitais, com foco particular na Bacia do Rio Tapajós. O projeto é financiado pela União Europeia.

A Rede MTI

A Rede de Monitoramento Territorial Independente (Rede MTI) é uma articulação que reúne mais de 70 organizações que atuam com monitoramento independente na Amazônia, incluindo lideranças comunitárias, organizações da sociedade civil e instituições de pesquisa.

O Monitoramento Territorial Independente é um instrumento por meio do qual povos e comunidades produzem conhecimento sobre seus territórios e modos de vida, identificando atividades produtivas, formas de manejo e transformações nos ecossistemas, além de impactos, ameaças e pressões.

A Rede MTI busca promover intercâmbios de experiências e facilitar a produção coletiva de conhecimentos, tendo como objetivo o fortalecimento das capacidades de monitoramento independente para a proteção de territórios e garantia de direitos na Amazônia. Desde 2020, é coordenada pelo FGVces em parceria com organizações que integram seu Conselho.



CONECTANDO...



Ei, parente, está sabendo que a Internet vai chegar no território, né?

A Internet é como um grande rio que liga várias comunidades, cidades e países do mundo todo. Assim como a gente usa o barco, a canoa e a rabeta para chegar aos lugares, na Internet usamos o celular, o computador ou até mesmo uma caixinha de sinal (roteador) para nos conectar e mandar mensagens, fazer chamadas de vídeo, ver vídeos, estudar e vender nossos produtos, como farinha, mel, artesanato e o peixe que a gente pesca.

Mas, do mesmo jeito que o rio tem lugar raso, correnteza forte e jacaré, na Internet também tem coisa boa e coisa perigosa. Por isso, é importante saber como navegar com cuidado, para não cair em armadilha e nem se perder nesse mundo. A Internet deve ser como um rio que nos leva aos lugares onde desejamos chegar.

Como podemos usar a Internet?

- Falar com a família e os amigos que moram longe.
- Estudar e aprender coisas novas.
- Vender o que se produz na comunidade.
- Assistir vídeos, ouvir música e brincar.
- Conhecer notícias de outros lugares.
- Conhecer outras pessoas, culturas e suas realidades.
- Mas também tem que se cuidar!

Na beira do rio, a gente aprende a respeitar as águas, não é? Na Internet é a mesma coisa: **é preciso ter cuidado para não cair em golpes digitais, ou para que as nossas informações pessoais não sejam roubadas.** Tem muita coisa boa, mas é preciso ter muita atenção. Por isso, é importante:

- Não contar a senha para ninguém.
- Não acreditar em tudo que vê ou lê.
- Não clicar em links estranhos, sem origem confiável.
- Cuidar do celular, para não emprestar para qualquer um.
- Conversar com a família ou com pessoas de sua confiança, caso tenha alguma dúvida.

Neste guia rápido, serão apresentadas algumas dicas de como usar a Internet com segurança. Muitos dos temas abordados neste material já fazem parte do dia a dia, como mandar mensagens no zap (WhatsApp), postar foto no Facebook ou no Instagram, fazer vídeo para o TikTok, e até divulgar o turismo comunitário ou a venda do que a comunidade produz.

Um tema importante são os cuidados que todo mundo deve ter para não cair em cilada, para respeitar outras pessoas e para fazer da Internet uma aliada, que ajude a comunidade, fortaleça as estratégias, que aproxime parentes, vizinhos e também traga novas amizades.

Bora navegar junto?

Se ajeita aí, que a viagem vai começar!



BEABÁ DO MUNDO DIGITAL

Para começar, vamos explicar algumas palavras que aparecem muito quando falamos de Internet.

Este quadro servirá como um glossário: é possível voltar aqui sempre que encontrar alguma palavra nova e for preciso tirar dúvidas.

Aplicativo (app)

Programa instalado no celular ou computador.

Tem aplicativo para escrever, fazer conta, tirar foto, ouvir música, mandar mensagem, entrar nas redes sociais, acessar serviço do governo, fazer compra, entre muitas outras funções.

Busca

Quando queremos encontrar algo na Internet, podemos usar uma ferramenta de busca. A mais conhecida é o Google, mas existem outras, como o Bing e o DuckDuckGo.

É só digitar o que está precisando saber e ela mostra os resultados.

A busca pode ser feita diretamente de um aplicativo no celular ou a partir de um navegador e é a forma mais fácil de encontrar algum site, informação ou conteúdo na Internet.

Chat (bate-papo)

É um espaço para conversar em tempo real com outras pessoas pela Internet. Em um chat, é possível mandar mensagem de texto, áudio, vídeo, figurinha... E tudo chega na mesma hora! O WhatsApp é um exemplo.

Cookies

São pequenos arquivos que os sites mandam para o nosso celular ou computador com a finalidade de guardar informações: os sites visitados, as compras feitas, as senhas salvas... Tudo isso pode tornar a navegação mais fácil e rápida em uma próxima vez.

Mas é importante ter cuidado! Alguns cookies guardam mais informação do que deveriam. É possível se resguardar ajustando as configurações de privacidade no navegador.

Dispositivo

Nome dado aos aparelhos usados para acessar a Internet, como celular, computador, tablet...

Download (pronúncia: *daunlôude*)

O processo de baixar um arquivo da Internet para o celular ou computador. Pode ser uma música, um vídeo, um documento, um aplicativo...

E-mail

Correio eletrônico, ou simplesmente e-mail, é como um correio via Internet. Serve para mandar e receber mensagens, fotos e arquivos. O endereço de e-mail é uma das formas principais para identificar usuários e permitir cadastros em redes sociais e outros sites. Todo endereço de e-mail tem o símbolo @ (arrouba), por exemplo: joao@provedor.com.

Link

Texto ou imagem que, ao clicar, leva direto para outra página da Internet. Pode ser um site, um vídeo, uma imagem ou outra informação.

No meio do texto, o link costuma aparecer com uma cor diferente e sublinhado. Algumas imagens também podem ser links — é só clicar e você é levado para outro lugar da rede.

Meme

Mensagem geralmente engraçada que se espalha pela Internet usando uma imagem ou vídeo.

Navegador (ou Browser)

É o programa usado para abrir páginas na Internet. Os mais conhecidos são o Chrome, Firefox e Safari.

Off-Line (pronúncia: *ofilaine*)

Quando a pessoa, o serviço ou o dispositivo não estão acessando a Internet ou não estão disponíveis na Internet, naquele momento. Sem sinal, sem conexão.

On-Line (pronúncia: *onlaine*)

Quando a pessoa, o serviço ou o dispositivo estão conectados e disponíveis para acesso via Internet.

Página e site (pronúncia: *saite*)

Uma página da Internet, ou página web, é como uma folha cheia de informações, mas no mundo digital. Pode ter texto, imagem, vídeo ou tudo isso junto. O acesso a essas páginas é feito com um navegador.

Já o site é como um caderno que reúne várias páginas em um mesmo lugar. Por exemplo, o site da Wikipedia tem muitas páginas sobre diferentes assuntos, como saúde, história, geografia, meio ambiente e cultura.

Post

É uma publicação realizada em redes sociais, na Internet, que pode incluir fotos, textos e vídeos. Postar é o ato de publicar um post.

Provedor

Empresa ou entidade que oferece a estrutura de comunicações necessária para acesso à Internet.

QR Code

QR Code é uma sigla para o termo em inglês “Quick Response Code”, que significa “código de resposta rápida”.

É uma espécie de código de barras que pode ser lido por celulares ou outros dispositivos que possuem uma câmera. Funciona para acessar informações de forma rápida, como sites, documentos, contatos e fotos.

Rede social

É um tipo de site que permite que as pessoas, comunidades e organizações se conectem e conversem.

São espaços online onde é possível compartilhar fotos, vídeos, mensagem, notícias e até fazer chamadas. Muitos são os usos das redes sociais: falar com os parentes e amigos, divulgar trabalhos e se atualizar, para ficar por dentro das novidades.

Exemplos de rede social são Facebook, Instagram, WhatsApp e TikTok.

Roteador (ou Router)

Aparelho que recebe o sinal da Internet e distribui para os celulares, computadores e tablets. Ele envia e recebe os dados que esses dispositivos usam para navegar online.

Spam

Mensagem que chega sem autorização, geralmente com propaganda. Os spams são enviados para muitas pessoas ao mesmo tempo, muitas vezes sem consentimento.

URL

URL é uma sigla em inglês que significa “Localizador Uniforme de Recursos”.

É o endereço usado para encontrar um site ou arquivo na Internet.

Por exemplo, <https://www.gov.br/> é o endereço da plataforma oficial do governo federal brasileiro. Para acessar essa plataforma, basta digitar esse URL no navegador.

NAVEGANDO: ALGUNS SITES RECOMENDADOS

Quer acessar conteúdos de qualidade sobre a Amazônia e outros temas importantes? Veja estas sugestões:

Amazônia Real

 <https://amazoniareal.com.br/>

Site com reportagens sobre a Amazônia, os povos da floresta, os territórios e os desafios da região.



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Agência Brasil

 <https://agenciabrasil.ebc.com.br>

Notícias sobre o que está acontecendo no Brasil e no mundo.



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Rede de Monitoramento Territorial Independente (Rede MTI)

 <https://www.redemti.org/>

Reúne diversos materiais e notícias sobre experiências de monitoramento territorial independente na Amazônia.



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Rede Conexão Povos da Floresta

 <https://conexaopovosdafloresta.org.br/>

Iniciativa que busca conectar em rede, através de Internet banda larga, povos e comunidades tradicionais da Amazônia, aliando conectividade e energia a programas de inclusão, segurança e empoderamento nas comunidades.



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Wikipedia

 www.wikipedia.org

Site colaborativo com explicações sobre praticamente tudo. Um bom ponto de partida para tirar dúvidas e aprender, desde que você confira as fontes indicadas em cada artigo.



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.



EXERCÍCIO 1:

Criando uma conta de e-mail

Ter uma conta de e-mail é importante para muita coisa: mandar mensagens, fazer cadastros, acessar aulas e usar redes sociais.

Para começar, é preciso escolher onde quer fazer seu e-mail. Os provedores mais usados aqui no Brasil são:



Outlook



Depois, é só seguir estes passos:

- Entre no site do provedor que você escolheu (ex: gmail.com)
- Clique em “Criar conta”
- Escolha um nome de usuário (ex: joaodasilva123@gmail.com)
- Crie uma senha segura (nada de usar “12345” ou o nome do cachorro)

Criar conta



Inscriva-se com o Google



Inscriva-se com o Facebook

OU

Email

johndoe@mail.com

Password

••••••••



Criar conta

Já possui uma conta? [Entrar](#)



Dica

Uma boa senha tem letras maiúsculas e minúsculas, números e símbolos.

EXERCÍCIO 2:

Fazendo uma busca no Google

Vamos aprender a usar o Google, uma ferramenta de busca que ajuda a encontrar informações sobre praticamente qualquer assunto.

- Vá até o Google www.google.com.
- Na barra de pesquisa, digite palavras relacionadas ao que você quer saber.

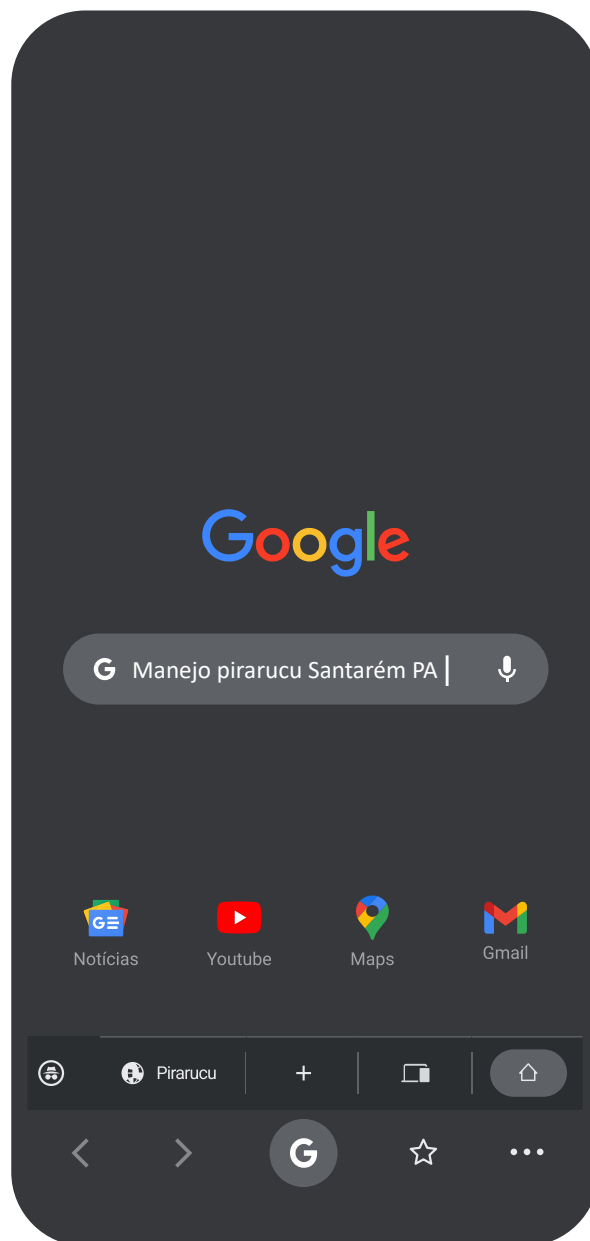
EXEMPLO

- Para saber mais sobre o manejo do pirarucu na região de Santarém (PA), podemos escrever: manejo; pirarucu; Santarém PA.
- Depois é só apertar o botão “Buscar” ou “Enter” e ver o que aparece.



Atenção

Antes de clicar em um site, certifique-se de que ele é seguro. Para mais informações, vá até a página 28.



EXERCÍCIO 3:

Instalando um aplicativo no celular

Vamos aprender como instalar um aplicativo de forma segura no celular.

● **No celular Android:** abra a loja Google Play Store, toque na barra de busca, digite o nome do aplicativo desejado e pressione Instalar.

● **No iPhone (iOS):** abra a App Store, toque na barra de busca, digite o nome do aplicativo desejado e pressione o ícone de obter ou instalar.



Dica

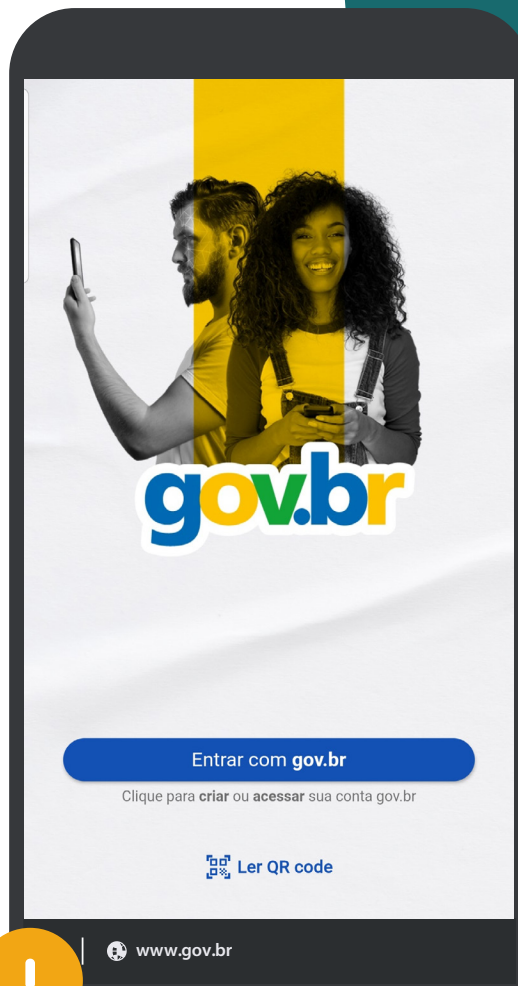
Antes de instalar, verifique se o aplicativo é oficial, conferindo o nome do desenvolvedor e as avaliações de outros usuários. Evite baixar aplicativos de links recebidos por mensagem ou de sites desconhecidos, pois eles podem conter vírus ou golpes.

EXERCÍCIO 4:

Criando sua conta gov.br

A conta gov.br é como um documento digital que prova que “você é você” quando vai usar serviços do governo pela Internet. Com ela, dá para fazer muita coisa sem precisar sair da comunidade: acessar serviços do SUS, pedir benefícios como o Seguro Defeso ou o Bolsa Verde, assinar documentos, consultar a Carteira de Trabalho e a CNH digital, se inscrever no ENEM, simular aposentadoria no Meu INSS, entre outros serviços.

- Entre no site www.gov.br ou instale o aplicativo gov.br e, depois, abra o app.
- Clique em “Entrar” e, depois, em “Crie sua conta gov.br”.
- Coloque o número do seu CPF e siga as orientações que vão aparecer.
- Escolha uma forma de validação: pelo aplicativo gov.br, por meio de bancos que fazem parte do sistema, por reconhecimento facial (usando a câmera) ou por código enviado no e-mail ou no celular.
- Crie uma senha forte, com letras maiúsculas e minúsculas, números e símbolos.



www.gov.br

Dica

Anote sua senha em um lugar seguro e nunca passe para outra pessoa. Sua conta é só sua.

**COMO USAR A
INTERNET DE FORMA
SAUDÁVEL?**



A Internet pode trazer muitos benefícios para o dia a dia: ajuda na comunicação com outras pessoas, na educação, na saúde, no trabalho e também no lazer. Mas é importante manter a atenção para os problemas que podem aparecer. A seguir, confira algumas armadilhas que existem no ambiente online e dicas importantes para navegar com mais segurança.

Crianças e adolescentes na rede

Os mais jovens costumam aprender rápido a mexer no celular e na Internet, não é? Parece que já nascem sabendo! Mas isso não quer dizer que podem ficar soltos na rede, sem orientação. A Internet é como uma rua ou uma praça bem movimentada: tem gente de todo tipo. Do mesmo jeito que é preciso ficar de olho nas crianças quando se vai para a cidade, também é preciso prestar atenção no que elas fazem no celular ou no computador. É importante conversar com os filhos, netos e sobrinhos. Pergunte que sites eles estão acessando, que vídeos estão assistindo, com quem estão conversando.

Também é indicado prestar atenção no tempo passado diante da tela, principal-

mente com os pequenos. Como ensinam os modos de vida tradicionais, crianças precisam correr, brincar, nadar no igarapé, conversar com a família e com os amigos, aprender com os mais velhos. Ficar tempo demais na Internet pode fazer mal à saúde. Os adultos devem manter atenção às mudanças de comportamento das crianças e adolescentes e sempre conversar com eles. O diálogo ajuda a entender o que está acontecendo e a mostrar caminhos mais seguros e saudáveis. Hoje em dia, existem aplicativos de controle parental que ajudam a acompanhar o que eles estão fazendo no celular e quanto tempo estão passando nas telas. Também é possível liberar ou bloquear alguns aplicativos, se for preciso. Alguns exemplos são os apps Google Family Link, AppBlock, Controle Parental Screen Time e Qustodio, disponíveis para Android e iOS.



Dica

As mesmas regras de respeito que valem na escola, na comunidade ou em casa também valem na Internet. Ofender alguém nas redes sociais ou durante um jogo online é tão desrespeitoso quanto fazer isso pessoalmente. É bom ficar atento: se um desconhecido puxar conversa na Internet, desconfie e tenha cuidado.

O Jogo

Existem muitos tipos diferentes de jogos. Alguns são só para passar o tempo, outros, quando bem usados, podem ajudar a treinar a memória, o raciocínio, a atenção e a criatividade. Mas é importante equilibrar: jogar um pouco e também variar com outras atividades.



Atenção

Alguns jogos têm conteúdo violento. Eles devem ser adequados à idade da criança ou do adolescente. E cuidado! Ultimamente têm aparecido muitos joguinhos na Internet que prometem dinheiro fácil, como o “Tigrinho”, as chamadas “bets” e outros jogos de aposta. Mas eles podem virar uma armadilha!

Jogos de azar têm grande capacidade de levar ao vício e causar efeitos muito sérios na vida das pessoas. Muita gente já perdeu todo o dinheiro jogando, entrou em dívida e adoeceu.

Por isso, ter cuidado é fundamental. Não caia na conversa de quem diz que dá para ganhar dinheiro fácil na Internet. Mesmo que você leve algum prêmio uma vez ou outra, a longo prazo uma coisa é certa: o jogo sempre ganha!

Conteúdo inadequado

No mundo digital, existe muito conteúdo considerado “pesado” e perturbador, principalmente para crianças e adolescentes. Não é difícil encontrar na Internet imagens violentas, ofensas, pornografia, mensagens que prejudicam a saúde, como o incentivo a parar de comer para emagrecer, jogos de azar e informações falsas. Esse tipo de publicação é chamado de conteúdo inadequado e inclui vários assuntos perigosos ou impróprios:

Conteúdo explícito e violento

São vídeos ou imagens com cenas violentas que circulam na Internet, como brigas, acidentes e assassinatos. Isso pode ser perturbador e causar problemas para a saúde mental das pessoas, especialmente para o emocional das crianças e dos adolescentes.

Conteúdo sexual

É aquele que mostra imagens ou vídeos com conteúdo pornográfico. A exposição a esse tipo de material não é adequada para menores de idade e pode atrapalhar o entendimento saudável sobre o corpo e a sexualidade.



Conteúdo ilícito

Na Internet tem ainda conteúdos que **violam as leis e as regras oficiais do país**. São publicações que mostram ou incentivam coisas proibidas, como compartilhamento ou venda de drogas, armas, abuso de crianças e adolescentes (pedofilia), extremismo e outras **ações criminosas**.

Incluem também **discursos de ódio e discriminação**, como mensagens ou postagens que promovem racismo, sexismo, homofobia, transfobia e outras formas de discriminação e ódio contra pessoas ou grupos.

Cyberbullying

Cyberbullying é uma palavra em inglês formada pela união de dois termos:

Cyber: relacionado ao mundo da Internet, das redes sociais e da tecnologia;

Bullying: atos de violência verbal, psicológica ou física, feitos de forma repetida e intencional, muitas vezes no ambiente escolar.

Infelizmente, são comuns casos de violência entre estudantes dentro das escolas. Mas nos últimos anos, com mais pessoas usando a Internet, esse tipo de agressão também passou a acontecer de forma online. Por isso, o nome cyberbullying.

O cyberbullying acontece quando alguém faz comentários ofensivos, ameaça ou persegue outra pessoa pela Internet, através de fóruns e redes sociais, como Instagram, TikTok, Whatsapp e outros espaços digitais.

Essas situações podem aparecer por meio de “memes”, imagens, vídeos e outros conteúdos compartilhados na Internet. É uma forma de agressão moral que tem o objetivo de atingir uma pessoa ou um grupo usando as ferramentas virtuais.

Essas ações podem causar muitos danos emocionais às vítimas e manter um ciclo de abuso dentro e fora das comunidades. São exemplos de cyberbullying:

- Espalhar mentiras e expor a imagem de alguém de forma constrangedora na Internet;
- Fingir ser outra pessoa e mandar mensagens ofensivas ou maldosas no lugar dela;
- Mandar mensagens ofensivas ou ameaças nas redes sociais, plataformas de jogos, sites e aplicativos de mensagens.

Phishing e golpes online

Apareceu uma mensagem “do nada” prometendo um trabalho de poucas horas ganhando muito? Ou um desconto daqueles imperdíveis, para comprar o seu produto dos sonhos por menos da metade do valor normal? Recebeu um e-mail pedindo confirmação de uma compra que você não fez? Ou uma mensagem dizendo que você precisa confirmar algo urgente?



Desconfie

Golpistas utilizam diversas iscas para atrair vítimas na Internet. Para se proteger dos golpes, é preciso ter atenção às informações que chegam por e-mails, mensagens de texto e propagandas em sites. Há muita informação falsa e maliciosa circulando nas redes.

Você já ouviu falar em Phishing?

Esse nome vem do inglês e quer dizer “pescaria”. Mas não é a pesca que os povos e comunidades tradicionais costumam fazer. Essa é uma pescaria perigosa, feita por gente mal-intencionada que usa a Internet para tentar “fisgar” nossas informações.

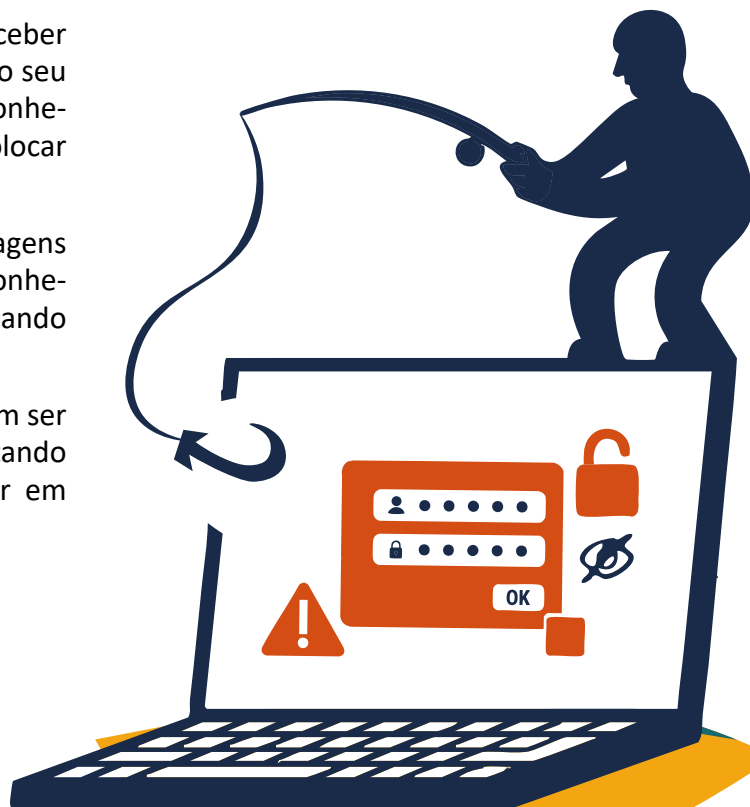
Esses criminosos se disfarçam de alguma entidade confiável, como banco, loja ou empresa conhecida e mandam mensagens no WhatsApp, por e-mail ou por rede social. Eles querem “pescar” nossas informações confidenciais, como senhas de banco, números de cartões de crédito e dados pessoais.

Como o phishing pode acontecer?

Geralmente, o phishing acontece por meio de e-mails, mensagens de celular ou sites falsos que parecem ser de empresas legítimas. Suspeite sempre que alguma mensagem ou site pedir seus dados pessoais.

EXEMPLOS

- **E-mails fraudulentos:** Você pode receber um e-mail enganoso que parece ser do seu banco ou de algum serviço que você conhece, pedindo para clicar em um link e colocar seus dados.
- **Mensagens de texto falsas:** Mensagens que parecem ser de uma instituição conhecida, solicitando informações ou indicando para clicar em um link suspeito.
- **Sites falsos:** Mensagens que parecem ser de uma instituição conhecida, solicitando informações ou indicando para clicar em um link suspeito.



Como se proteger dos perigos da Internet?

Existem muitos riscos e ameaças no mundo virtual. Por isso, é importante cuidar das informações pessoais e aprender maneiras seguras de navegar:

Use senhas fortes

Ter uma senha difícil é como trancar bem a porta da nossa casa. Senhas longas, com letras, números e símbolos, são mais seguras e difíceis de adivinhar. Elas dificultam invasões de contas na Internet, sejam as contas pessoais de e-mail, de WhatsApp, ou mesmo os aplicativos bancários.

Cuidado para não repetir a mesma senha em tudo. E não compartilhe com ninguém. Senha é segredo!



Cuidado com compras online e operações bancárias

- Antes de comprar alguma coisa pela Internet, confira se a loja é de confiança e se você está no site oficial;
- Antes de mandar um Pix, confira o nome e os dados de quem vai receber. Só confirme se tiver certeza de que é a pessoa certa;
- Recebeu mensagem de parente ou amigo pedindo dinheiro? Não mande na hora. Primeiro ligue para a pessoa ou tente falar de outro jeito, para saber se é ela mesma. Pode ser golpe.

Verifique a origem das mensagens

Nem tudo que chega no celular ou no e-mail é verdade. Ao receber algo, sempre confira o endereço de e-mail e o número de contato de quem mandou.

Empresa séria de verdade não pede senha, CPF ou outros dados pessoais por mensagem de texto, WhatsApp ou e-mail.

Se parecer estranho, é melhor não responder.



Não clique em links suspeitos

Antes de clicar em um link, analise o contexto e os detalhes. **Se tiver dúvidas, não clique!**

Se precisar acessar um site, é melhor digitar o nome direto no navegador ou pedir ajuda para alguém de confiança.

Ao pesquisar no Google ou em outro site de busca, veja se o endereço (URL) do site está correto e **verifique se a conexão é segura**.

Os sites mais seguros começam com “https”, com um “s” no final, ao invés de “http”.

Use verificação em duas etapas

A verificação em duas etapas, ou autenticação de dois fatores, é uma camada a mais de segurança para confirmar que somos nós mesmos que estamos usando a nossa conta.

Quando ativamos essa proteção, precisamos incluir uma segunda informação, além da senha, para conseguirmos fazer o login. Pode ser por meio de um código enviado por mensagem, perguntas secretas, impressão digital, reconhecimento facial, etc.

SEGURO

 https://



NÃO SEGURO

 http://



Isso dificulta a invasão das contas, mesmo se souberem a senha. Para ativar esse recurso, basta acessar as configurações de e-mail, das redes sociais e de outras contas, e selecionar: “verificação em duas etapas” ou “autenticação em dois fatores”. Normalmente essa funcionalidade está localizada na seção “Segurança”.

Use antivírus no seu celular, computador ou tablet

O antivírus, ou antimalware, é fundamental para proteger os aparelhos contra vírus e outras ameaças virtuais, como os ataques de phishing. Instalar e manter o antivírus sempre atualizado ajuda a garantir uma defesa eficaz contra esses perigos.

Cuide da sua privacidade na Internet

Assim como não contamos nossa vida para qualquer um, na Internet também é bom tomar cuidado com o compartilhamento de certas informações.

- Não forneça seus dados pessoais em sites desconhecidos ou que pareçam estranhos.
- Ao preencher um cadastro online, inclua apenas informações que forem realmente necessárias.
- Preste atenção nas permissões que os aplicativos pedem, como acesso à câmera, microfone, localização e contatos. Dê permissão apenas para o que for preciso.

- Quando entrar em um site e aparecer a mensagem sobre cookies, escolha “recusar” ou “aceitar só os essenciais”. Isso ajuda a diminuir a quantidade de informações que o site guarda sobre você.
- Nas redes sociais, ajuste as configurações de segurança e privacidade e pense bem antes de aceitar contatos de pessoas que você não conhece;
- Proteja também a privacidade das crianças: evite postar fotos ou informações sobre elas nas redes sociais;
- Quanto menos informação sua na Internet, melhor para sua segurança.

Boatos e notícias falsas

Qualquer pessoa pode **publicar** conteúdo na Internet. Mas nem tudo o que circula pelas redes é verdade. Aliás, muita coisa é só boato, ou mentira mesmo.

Tem muitos tipos de boato por aí. A notícia falsa, que muita gente chama de fake news, é um **boato que tenta se passar por notícia verdadeira**. Ela é feita para parecer que saiu de um jornal sério ou de um canal confiável, por isso é fácil se enganar.

Não acredite em tudo o que se vê ou ouve nas redes. Boatos e informações falsas podem fazer você cair em golpes e levar a pensar ou agir conforme os interesses de outras pessoas.

COMO RECONHECER UM BOATO?

Use o bom senso: às vezes, basta a gente refletir um pouco para perceber que a mensagem que recebemos é um boato, ou que a notícia que estamos lendo não pode ser verdadeira.

Antes de acreditar, **pense bem: essa história faz sentido?** Muitos boatos...

- têm título chamativo, alarmista ou apelativo

- são encaminhados com frequência, em vários grupos
- pedem para ser bastante compartilhados
- não mostram quem escreveu nem de onde veio a informação
- usam notícia velha como se fosse atual e imagem fora de contexto
- apresentam fatos sem evidências, ou seja, não mostram provas do que estão falando
- tentam se passar por notícia verdadeira

QUER SABER SE É VERDADE?

- vá direto à fonte da notícia, veja se ela foi divulgada por um canal verdadeiro ou um site oficial
- veja se tem algum texto ou comunicado desmentindo a notícia ou o boato
- confira a data da notícia e dos fatos
- não veja apenas os títulos, leia tudo com atenção

Vídeos, imagens e áudios falsos

Hoje em dia, dá para modificar imagem, vídeo e até voz com programas de computador e inteligência artificial. Às vezes pode parecer que alguém falou ou fez algo que, na verdade, nunca aconteceu. Pode ficar tão bem-feito que a gente se engana fácil.

Se o conteúdo parecer suspeito, faça uma busca para confirmar se é verdadeiro ou se alguém já desmentiu a informação.

As imagens e vídeos falsos podem ter pequenos defeitos. Por isso, repare se:

- a boca da pessoa no vídeo não acompanha o que ela está falando
- os olhos não piscam direito ou a imagem parece estranha
- a voz parece forçada

Se receber áudios com vozes parecidas com as de pessoas conhecidas, preste atenção: a voz tem a emoção ou o jeito de falar que combina com a pessoa e com o assunto?

COMO COMBATER BOATOS E FAKE NEWS?

- **Não compartilhe boatos:** Ao suspeitar que uma notícia é falsa, não repasse adiante! Quanto mais um boato circula, mais pessoas vão acreditar nele.
- **Verifique todo o conteúdo antes de compartilhar uma notícia.** Pense: “será que isso é verdade? Será que vale mesmo espalhar?”
- **Orienta outras pessoas** a não compartilharem boatos.



COMUNICADO

Esta seção adaptou conteúdo produzido pelo CERT.BR



Confira o fascículo completo pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

EXERCÍCIO 3:

Descubra se a informação é verdadeira ou falsa

Vamos exercitar um pouco do que aprendemos sobre os boatos e *fake news*?

Sabe aquelas mensagens que são compartilhadas muitas vezes e em vários grupos de WhatsApp? Escolha uma e faça o teste: verifique se ela é verdadeira ou falsa.

Alguns sites disponíveis na Internet podem ajudar você nesse trabalho. Eles verificam se algumas das informações mais circuladas pelas redes sociais são fato ou fake:

🔍 <https://lupa.uol.com.br/>

🔍 <https://www.aosfatos.org/>

🔍 <https://www.boatos.org/>

🔍 <https://noticias.uol.com.br/confere/>

🔍 <https://g1.globo.com/fato-ou-fake/>

Por que esses cuidados são importantes?

Quando aprendemos formas mais seguras de usar a Internet, conseguimos aproveitar muito mais as oportunidades que o mundo digital nos oferece.

Com essas medidas de proteção online, as comunidades e aldeias ganham mais segurança e podem exercer a cidadania: estudar, vender produtos, ter acesso à saúde e a outros serviços públicos, divulgar sua cultura e história, além de disseminar informações sobre suas lutas.

Na Amazônia, a Internet e a tecnologia têm ajudado muita gente a olhar e a cuidar do território, usando equipamentos digitais para fazer vigilância, denunciar invasão, acompanhar o desmatamento e proteger seus modos de vida. Se você quiser conhecer mais sobre como utilizar essas ferramentas e a conectividade na defesa dos territórios tradicionais, consulte o “Guia Rápido: Monitoramento Territorial Independente e Tecnologias Digitais”, também produzido pelo projeto INDICA Tapajós, do FGVces e da Sapopema.



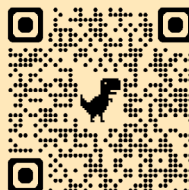
PARA SABER MAIS

Este guia rápido foi construído com base nos materiais e documentos listados abaixo.

Quer navegar na Internet com mais segurança? Escaneie os QR Codes e explore mais dicas e cuidados:

Canal Cidadão na Rede (youtube). Produção NIC.BR

 <https://www.youtube.com/playlist...>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Cartilha de Segurança para Internet – Fascículos. Produção CERT.BR, NIC.BR e CGI.BR

 <https://cartilha.cert.br/fasciculos>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Proteção de crianças e adolescentes na Internet: recomendações para pais e responsáveis – Produção Governo Federal, 2020.

 <https://www.gov.br/mdh/pt-br/navegue-por-temas/crianca...>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Internet segura para seus filhos. Produção CERT.BR, NIC.BR e CGI.BR – 2ª Edição, 2022.

 <https://internetsegura.br/pdf/guia-internet-segura-pais.pdf>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Celular não é vilão, mas é preciso saber usar. Por Joanna Cataldo e Mayara Penina do COLO – Coletivo de Jornalismo Infantojuvenil. Produção Revista Casa Comum, 2025.

 <https://revistacasacomum.com.br/...>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.

Cuidados Digitais. Produção Escola de Ativismo.

 <https://escoladeativismo.org.br/cuidados-digitais/>



Acesse diretamente pelo QR Code

Aponte a câmera do seu celular para a figura ao lado.



Produção técnica



Apoio



Financiado pela
União Europeia

