GUIA RÁPIDO DE BOAS PRÁTICAS PARA USO DA WEB

Realização

CONEXÃO POVOS da FLORESTA

cewebbr nicbr cgibr

Apoio

UK Government

FICHA TÉCNICA

GUIA RÁPIDO DE BOAS PRÁTICAS PARA USO DA WEB

SOBRE ESTA PUBLICAÇÃO

Programa de Acesso Digital da Embaixada Britânica no Brasil (Digital Access Programme – DAP)

GUIA RÁPIDO DE BOAS PRÁTICAS PARA USO DA WEB E SEGURANÇA DIGITAL

O guia rápido de boas práticas para uso da Web e segurança digital é uma das iniciativas do Programa de Acesso Digital da Embaixada Britânica no Brasil (Digital Access Programme – DAP), financiado pelo Governo Britânico, em parceria com o Conexão Povos da Floresta e o Centro de Estudos sobre Tecnologias Web (Ceweb.br) do NIC.br.

PARCERIAS

- Centro de Estudos sobre Tecnologias Web (Ceweb.br) do NIC.br
- Embaixada Britânica no Brasil - por meio do Programa de Acesso Digital
- Instituto Conexão Povos da Floresta (ICPF)

COORDENAÇÃO

Centro de Estudos sobre Tecnologias Web (Ceweb.br) do NIC.br

GERENTE

Vagner Diniz

REDAÇÃO

Amanda Marques , Diogo Cortiz, Ewerton da Silva, Reinaldo Ferraz, Selma Morais e Tatiana Del Gadelha

REVISÃO GERAL

Ewerton da Silva, Selma de Morais e Vagner Diniz

DIAGRAMAÇÃO

Larissa Paschoal (Assessoria de Comunicação do NIC.br)

ILUSTRAÇÕES

Freepik.com e Shutterstock

Realização

CONEXÃO POVOS da FLORESTA

ceweb.br nic.br cgi.br

Apoio

UK Government

INTRODUÇÃO

O uso consciente da Web sempre foi uma preocupação constante do Grupo de Trabalho (GT) Educação do Conexão Povos da Floresta. Embora a ampliação do acesso à Internet em comunidades indígenas, quilombolas, ribeirinhas e extrativistas seja fundamental, é igualmente importante compreender o funcionamento da Web e estar atento a questões como segurança, privacidade e uso responsável. Esses aspectos são essenciais para garantir o aproveitamento adequado dos recursos promovidos pelo projeto.

O GT Educação já formou dezenas de facilitadores no Programa Sabedoria Digital. No entanto, identificamos a necessidade de disponibilizar conteúdos complementares, de fácil acesso, principalmente sobre segurança e privacidade, temas amplamente levantados pelos comunitários dos encontros online, presenciais e aulões. Essa demanda evidencia não só o interesse das comunidades, mas também é uma ótima oportunidade para reforçar cuidados essenciais que devem permanecer no radar de todas as comunidades conectadas pelo Projeto.

A parceria entre o Governo Britânico, o Conexão Povos da Floresta e o Centro de Estudos sobre Tecnologias Web (Ceweb.br) do NIC.br, visa a cooperação para o desenvolvimento de habilidades no uso adequado, seguro e responsável da Internet pelas comunidades.

Este guia é livre e gratuito, podendo ser compartilhado livremente desde que se faça referência aos autores. É uma forma do programa compartilhar conhecimento com toda a sociedade e garantir a sua disseminação e reconhecimento Sugestão de citação no padrão ABNT:

> Centro de Estudos Sobre Tecnologias Web Ceweb.br. **Guia rápido de boas práticas para uso da Web e segurança digital**. Produção: Programa de Acesso Digital da Embaixada Britânica no Brasil (DAP). Parceria: Governo Britânico, Instituto Conexão Povos da Floresta e NIC.br. São Paulo: NIC.br, 2026.

Em citações no corpo de texto:

Citação Indireta (Autoria no texto): Segundo o Centro de Estudos sobre Tecnologias Web (Ceweb.br) (2026), a segurança digital deve ser...

Citação Direta (Autoria entre parênteses, ao final da frase): "Trecho extraído do guia..." (Ceweb.br, 2026).

Para obter mais informações sobre o projeto e as capacitações oferecidas entre em contato com a Equipe do Conexão Povos da Floresta, que possui diversos grupos de trabalho. Para conhecer mais sobre os grupos e o trabalho desenvolvido pelo ICPF, acesse a página do projeto: **https://conexaopovosdafloresta.org.br/contato/**.

Realização

Apoio

BOAS PRÁTICAS PARA USO DA WEB

A conectividade traz muitos benefícios, mas também alguns riscos. Você sabe quais são eles?

NAVEGANDO NA WEB

A conexão com a Internet permite que as pessoas acessem o ambiente digital e usufruam de diversas oportunidades. Por meio dela, é possível realizar atividades do dia a dia com mais facilidade, como acessar serviços públicos, utilizar bancos, fazer compras e participar de capacitações e buscar atendimento ou informações de saúde. A Internet amplia o acesso a uma variedade de produtos e serviços sem a necessidade de deslocamento, algo importante e completo quando pensamos em muitas regiões da Amazônia. Quando você abre um vídeo, manda mensagem ou consulta um serviço do governo, seu pedido viaja por um caminho longo até nos trazer as informações que buscamos. Essas informações chegam até nós por meio de um navegador ou aplicativo, assim temos acesso a conteúdos de todo o mundo.

Tudo o que acessamos na Web está armazenado em um computador em algum lugar do planeta conectado a essa rede mundial, a Internet. Cada ação executada, como pressionar um botão, acessar um *link* ou baixar um arquivo envia uma requisição do seu celular para o roteador, que vai para a antena, que dispara esse pedido para satélites em volta da Terra, que trocam informações entre si até localizar o satélite mais próximo do computador que tem a informação que precisa. Depois de recebida a requisição, o computador manda de volta a resposta que você solicitou. Tudo isso em fração de segundos!

Apesar da familiaridade com dispositivos como celulares e tablets, nem sempre sabemos tudo sobre o uso da Internet. As páginas e aplicativos costumam ser bem intuitivos, mas algumas técnicas nós só descobrimos conforme vamos usando mais a rede e buscando informações em locais confiáveis. Por exemplo, você sabia que manter o dedo pressionado em algum elemento da página, como *link*, imagem ou texto abre um menu de ações cheio de recursos adicionais, como a possibilidade de copiar, colar, compartilhar e exportar esse conteúdo selecionado?

Realização

CONEXÃO POVOS da FLORESTA

ceweb.br nic.br cgi.br

Apoio

UK Government

SEGURANÇA E PRIVACIDADE *ONLINE*

O mundo *online* é repleto de possibilidades. Navegar, jogar, ouvir música e muitas outras experiências estão disponíveis na palma da nossa mão.

Por isso precisamos ter cuidado ao navegar e ao compartilhar nossos dados na rede. É essencial conhecer os riscos e saber como nos proteger no ambiente digital.

Existem diversas situações que envolvem a segurança ou exposição dos nossos dados, como por exemplo:

- Alguém divulga informações sobre você ou imagens onde você está presente, sem a sua autorização prévia;
- Um impostor se faz passar por você, cria um e-mail ou perfil falso em seu nome e o utiliza para coletar informações pessoais sobre você;
- Alguém acessa suas redes sociais, dados bancários e pessoais para cometer fraudes e outros tipos de crimes;

Isso pode:

- Comprometer a sua privacidade, de seus amigos e parentes Facilitar o furto da sua identidade
- Facilitar a invasão de suas contas de usuário
- Causar perdas financeiras, perda de reputação e até mesmo falta de crédito
- Colocar em risco a sua segurança no mundo real, fora das telas
- Favorecer o recebimento de spam (e-mails de propagandas)

Por isso alguns cuidados são fundamentais para melhorar nossa segurança na Internet e fora dela. Ao longo deste material você entenderá melhor o que e quais são esses riscos, como se proteger e como orientar as pessoas ao seu redor sobre como se prevenir deles.

Realização

CONEXÃO POVOS da FLORESTA

cgi.br nic.br cgi.br

Apoio

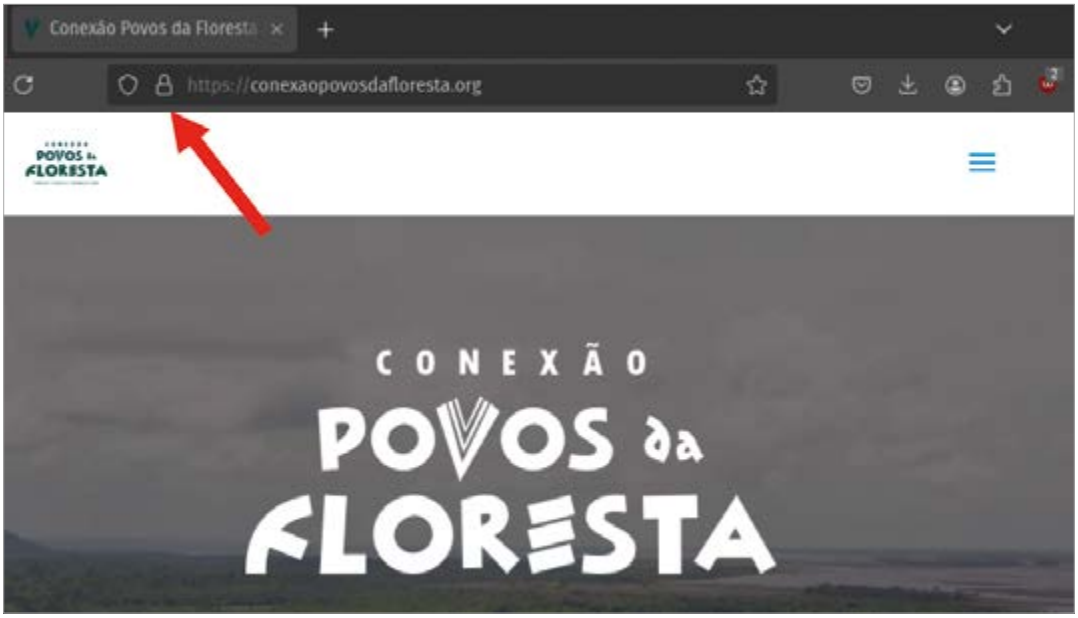
UK Government

CUIDADOS DURANTE A NAVEGAÇÃO *ONLINE*

Quais cuidados devemos ter para evitar esses riscos?

VERIFIQUE SE O *SITE* TEM CERTIFICADO DE SEGURANÇA

O certificado de segurança ("o cadeado" na barra de endereço do *site*) é o símbolo que aparece sempre ao lado do endereço do *site* na barra superior do navegador. Alguns navegadores mostram como um símbolo de cadeado, outros utilizam símbolos diferentes. Isso significa que os dados que estão sendo transmitidos são "embaralhados" durante a transmissão e isso dificulta o acesso de pessoas não autorizadas que tentam acessar essas informações no caminho. Isso vale para todos os tipos de *sites* que você precisa inserir algum dado, desde um serviço público até um *site* de compras *online*.



Quando você toca nesse símbolo, uma série de informações sobre a página são exibidas, inclusive sobre a segurança da página.

VERIFIQUE O NOME DO *SITE* QUE ESTÁ NAVEGANDO

É muito comum que golpistas utilizem endereços de *sites* falsos para enganar as pessoas. Eles podem usar nomes muito parecidos com os de instituições reais. Preste sempre bastante atenção ao nome do *site* que aparece na barra de endereços para se certificar que esse é o que você realmente estava procurando. Desconfie se notar diferenças como a falta de letras, a troca de letras por número,se o endereço do *site* parece uma brincadeira, ou se o final do *site* não condiz com o seu conteúdo (exemplo: um *site* supostamente do governo, que não termine com gov.br.).

VERIFIQUE SE OS *LINKS* LEVAM AO ENDEREÇO CORRETO

Especialmente em *links* recebidos por e-mail ou redes sociais, sempre verifique se o *link* envia para o endereço correto. No celular ou tablet, você pode verificar isso mantendo o dedo pressionado sobre o *link* por alguns segundos. Essa informação aparece na parte superior do menu.

Realização

Apoio

- **Situação real:** alguém recebe no WhatsApp "consulta de benefício / cadastro / boleto" com *link*.
- **Boa prática:** olhar o endereço com calma, evitar clicar em *link*s da mensagem; entrar pelo app oficial da suposta organização que está em contando ou ainda digitar o endereço do *site* no navegador.
- **Se não fizer:** ao clicar no *link* recebido, você poderá cair em páginas falsas, e ao informar CPF/senha, alguém pode usar os seus dados para realizar atividades indevidas com eles, como por exemplo, abrir uma conta bancária e solicitar empréstimo(s) em seu nome; realizar compras sem seu conhecimento etc.

CUIDADO COM *LINKS* ENCURTADOS

*Link*s encurtados são utilizados para reduzir o número de caracteres da mensagem, mas podem esconder um endereço com código malicioso. Desconfie de *link*s encurtados publicados em redes sociais ou enviados por WhatsApp.

- **Situação real:** fazer download de filmes/séries por meio de *site* suspeito.
- **Boa prática:** evite o download ilegal e *site*s "de filme grátis"; oriente a seus parentes que essa prática pode causar problemas burocráticos para sua comunidade.
- **Se não fizer:** risco de aviso/bloqueio do serviço e perda de conectividade para todos, além da possibilidade de "baixar" um vírus escondido.

NÃO BAIXE CONTEÚDO PROTEGIDO POR DIREITOS AUTORAIS

Muitos conteúdos, como filmes, música e livros, podem ser protegidos por direitos autorais. São conteúdos vendidos por plataformas específicas e muitas vezes tem recursos de verificação se está sendo baixado de forma ilegal.

Isso gera um enorme problema para os usuários do Conexão Povos da Floresta, pois os termos do serviço da Star*link* não permitem que a Internet fornecida por eles seja usada para download de conteúdo protegido por direitos autorais.

Segundo os termos da empresa:

> *"Faz parte da nossa política o encerramento da conta de violadores recorrentes de direitos autorais nos casos aplicáveis."*
>
> *Fonte: Starlink.com*

Isso significa que o acesso a Internet na comunidade pode ser encerrado caso os usuários baixem conteúdo protegido por direitos autorais. Alguns facilitadores reportaram ter recebido alertas da Star*link* de conteúdo ilegal baixado pela rede. A Starlink complementa em sua documentação que em caso de reincidência após os alertas o serviço pode ser encerrado. Para que isso não ocorra, evite este comportamento e alerte seus parentes.

CUIDADOS DURANTE COMPRAS *ONLINE*

PESQUISE SE O *SITE* É CONFIÁVEL

Verificar se o símbolo de segurança mencionado anteriormente aparece no seu *site* preferido de compras é muito importante, pois você não vai apenas navegar no *site*, mas também irá inserir dados pessoais e possivelmente até dados bancários ou de cartão de crédito. Se durante o processo de compra alguma página não tiver esse símbolo, não conclua a compra.

Uma rápida busca *online* pode trazer uma série de informações sobre a loja, especialmente se ela tem muitas reclamações de que não entrega produtos ou de pessoas que sofreram golpes. Normalmente essas lojas falsas são usadas para golpes, pois anunciam produtos muito mais baratos do que o preço regular. Utilize ferramentas como o *site* "Reclame Aqui!" e a página "*Site* Confiável" para fazer essa pesquisa.

DESCONFIE DE PROMOÇÕES ABSURDAS

Hoje temos uma série de ferramentas para pesquisar preços e produtos em diversas lojas. É comum encontrarmos uma variação de preços, porém algumas lojas podem colocar valores muito abaixo ou fazer promoções boas demais para serem verdadeiras. Na dúvida, pesquise sobre a loja e sobre a promoção antes de efetuar a compra.

- **Situação real:** você recebeu um anúncio para a compra de um celular "muito barato" ou para compra de uma peça de motor de rabeta muito abaixo do valor médio de mercado.
- **Boa prática:** pesquise o nome da loja e reclamações antes; compare preço em 2 ou 3 lugares.
- **Se não fizer:** você pode pagar e não receber o produto ou serviço; ou recebe um produto falsificado; e ainda entrega dados financeiros e do seu cartão do banco/crédito que poderá lhe trazer ainda mais prejuízos.

EVITE SALVAR OS DADOS DO CARTÃO DE CRÉDITO NO *SITE*

Apesar de ser um recurso que facilita compras futuras, salvar os dados do cartão de crédito nos *site*s pode facilitar o uso por golpistas que conseguiram acesso a sua conta. Prefira fazer uso de cartões virtuais de uso único ou temporário. Geralmente os aplicativos de banco oferecem a opção de gerar esses cartões virtuais.

ATIVE NOTIFICAÇÕES DE COMPRA POR CARTÕES (*SITE* OU APP DO BANCO OU CARTÃO)

Esse recurso permite que você seja notificado caso uma compra seja feita em um *site* ou aplicativo, porém golpistas costumam enviar mensagens em massa informando de compras feitas para que possam obter seus dados. Se você receber uma ligação ou mensagem quando não fez compras, desconfie e entre em contato com o *site* ou banco pelos canais oficiais disponibilizados na parte de trás dos seus cartões, nunca por *link*s ou telefones contidos na mensagem.

Realização

CONEXÃO POVOS da FLORESTA

ceweb.br nic.br cgi.br

Apoio

UK Government

CUIDADOS NAS REDES SOCIAIS

NÃO ABRA *LINKS* ENVIADOS POR REDES SOCIAIS

É muito comum golpistas utilizarem redes sociais e comunicadores instantâneos (como WhatsApp e Telegram) para tentar enviar golpes. Eles utilizam *link*s com *site*s falsos ou com códigos maliciosos que podem infectar o seu celular e permitir o acesso pelo golpista e até danificar o seu celular.

Lembre-se: A Internet é de uso comunitário, quando um celular é infectado por vírus, pode mandar mensagens sozinho e pode atrapalhar a Internet de todos , pois sobrecarrega a rede.

Os golpistas têm enviado mensagens em nome de bancos, dizendo que uma compra foi aprovada, ou que você tem crédito ou até empréstimo. Se desconfia da mensagem, entre em contato pelos canais oficiais do banco (nunca por telefone, e-mail ou *link* que está na mensagem suspeita).

Quando alguém cai em um golpe e o criminoso passa a ter acesso aos seus contatos ou grupos, o problema pode se espalhar e atingir outras pessoas, não apenas você.

NÃO ABRA ARQUIVOS ENVIADOS POR DESCONHECIDOS

Em alguns golpes as pessoas enviam arquivos como se fossem documentos ou fotos, porém o arquivo pode ser um software malicioso que vai comprometer seu celular ou computador. Desconfie sempre! Se possível, peça para a pessoa digitar ou mandar um áudio explicando o conteúdo do arquivo enviado.

- **Situação real:** você recebe um "documento da prefeitura / comprovante / foto" em arquivo.
- **Boa prática:** peça explicação por áudio e confirme quem enviou; não abra se não tiver certeza.
- **Se não fizer:** o celular pode ser contaminado com um programa malicioso e começar a roubar o dinheiro de suas contas de banco cadastradas no dispositivo, mandar diversas mensagens em massa sem sua autorização e até travar.

CUIDADO AO POSTAR SUA ROTINA E LOCALIZAÇÃO

É comum pensarmos que o ambiente digital é 100% seguro e apenas cercado de parentes, amigos e conhecidos nas redes sociais. Mas no caso de perfis públicos ou se alguém mal-intencionado acessa a rede social de um conhecido seu para coletar suas informações, sua segurança poderá estar comprometida.

- **Situação real:** postar "indo pra cidade tal dia", foto da comunidade, da canoa, do rio, do documento.
- **Boa prática:** evite mostrar a localização, documentos, placas, rotinas e bens de valor.
- **Se não fizer:** facilita golpe, extorsão, furto ou gente mal-intencionada "mapeando" a sua rotina.

Atenção redobrada com as crianças: evite postar fotos de crianças com o uniforme escolar, ou outros elementos que indiquem sua rotina e localização.

DESCONFIE DE QUEM NÃO ESTÁ NA SUA LISTA DE CONTATOS

Um golpe muito comum é uma pessoa se passar por alguém da sua família, colocar foto no perfil e pedir dinheiro por pix. Nesse caso, a recomendação é procurar pela pessoa na sua lista de contatos e ligar ou mandar mensagem

Realização

Conexão Povos da Floresta · ceweb.br · nic.br · cgi.br

Apoio

UK Government

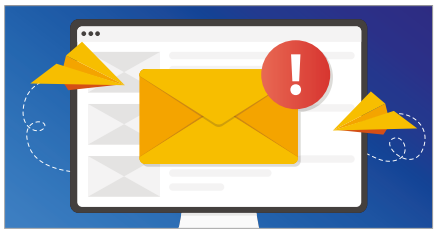
para o número que você tem salvo. Não faça nenhum pagamento ou transferência sem ter certeza se aquela pessoa é realmente quem está dizendo ser.

- **Situação real:** você recebe uma mensagem de um número desconhecido de um parente "Oi, estou com número novo, faz um Pix urgente."
- **Boa prática:** ligar para o número antigo da pessoa, ou pedir áudio/vídeo com uma informação que só a pessoa saberia.
- **Se não fizer:** o seu dinheiro vai para o golpista e depois pode ser muito difícil de recuperar.

CUIDADOS COM SEU E-MAIL

O e-mail é muito importante para o seu dia a dia digital. Com ele você pode se comunicar com pessoas e empresas e criar contas em lojas *online*, redes sociais e até no Gov.br, usufruindo dos serviços, auxílios e benefícios disponibilizados por lá. Você também precisa de um e-mail para usar o celular. Tanto Android como IOs exigem a criação de uma conta para uso do dispositivo. Por isso sua conta de e-mail e senha devem ser bem protegidas.

CUIDADO COM *LINKS* E ARQUIVOS RECEBIDOS POR E-MAIL



Mensagens de e-mail podem conter *link*s ou arquivos maliciosos que podem comprometer o uso do seu computador ou celular. Os *link*s podem mandar para páginas falsas e os arquivos podem instalar vírus e comprometer seu dispositivo.

Sempre desconfie de mensagens com *link*s e anexos. É comum que golpistas usem modelos de mensagens de bancos, lojas virtuais e até de sistemas de governo para enganar o usuário. As mensagens costumam vir com *link*s ou arquivos para solucionar algum problema com a sua conta.

Bancos, empresas e governos costumam fazer diversas comunicações alertando que nunca enviam *link*s, arquivos ou pedem senha por mensagem ou e-mail. Se você desconfia do e-mail que recebeu, entre em contato pelos canais oficiais da instituição bancária.

VERIFIQUE O REMETENTE DA MENSAGEM

Desconfie de mensagens com e-mails que não fazem parte da instituição identificada na mensagem. Um banco nunca mandaria uma mensagem com o endereço de e-mail "contato@gmail.com" ou "meubanco@tgjprtp.px".

Porém, os golpistas conseguem "mascarar" o endereço de e-mail e fazer com que pareça realmente um e-mail com nome e servidor oficiais. Mesmo recebendo uma mensagem de "segurança@seubanco.com.br", nunca abra *link*s ou arquivos por e-mail.

Lembre-se: Os bancos nunca pedirão sua senha por ligação, mensagem ou e-mail e não pedem para acessar *link*s na mensagem de SMS ou WhatsApp.

Realização
CONEXÃO POVOS da FLORESTA
cgi.br nic.br cgi.br
Apoio
UK Government

CUIDADOS COM SUAS SENHAS

NÃO USE DADOS PESSOAIS NA CRIAÇÃO DA SENHA

Evite criar senhas com dados pessoais de fácil identificação. Datas de nascimento, nome de mãe, pai ou filhos, cônjuges podem ser senha fáceis de serem descobertas, especialmente se o golpista conhece sua rotina.

NÃO USE SENHAS COMUNS

Senhas como "abc123", "teste123", "mudar", "admin" são senhas simples e que estão amplamente espalhadas na Internet. Os golpistas usam um recurso de "colheita" e pegam da Internet milhões de senhas comuns e tentam usar em vários sistemas. Se eles encontram algum sistema com uma senha assim eles conseguem acesso e podem causar problemas nas contas invadidas. Nomes de artistas e esportistas famosos também entram na categoria de senhas comuns, então evite seu uso.

CRIE SENHAS LONGAS E COM DIVERSOS CARACTERES

Senhas curtas são fáceis de serem descobertas. Para tornar as senhas mais difíceis de serem descobertas faça uso de caracteres especiais, como "!", "@", "#" dentre outros. Combine também letras maiusculas e minúsculas e adicione números. Isso torna a senha muito mais segura. Hoje os sistemas já exigem senhas mais longas e com caracteres especiais, maiusculas e números, então faça uso desse recurso.

Exemplo de senha segura: P@v0sdaf100r&st@!

Viu como essa senha consegue misturar números, letras e caracteres especiais? Não utilize exatamente essa, mas crie uma que também faça uso de todos esses elementos diferentes.

Também é importante ter senhas diferentes para cada serviço e rede social.

- **Situação real:** uso da mesma senha para o Facebook e para o e-mail.
- **Boa prática:** use senhas longas, de preferência em forma de frase, e diferentes para cada serviço (como e-mail e redes sociais). Além disso, ative a verificação em duas etapas: assim, além da senha, será necessário confirmar que é você quem está acessando, aumentando a segurança da sua conta.
- **Se não fizer:** se uma senha vazar, o golpista pode acessar várias contas suas, como redes sociais, e-mail e até serviços bancários. Isso abre muitas portas para golpes e pode causar grandes problemas, permitindo que ele realize ações que prejudicam você, seus parentes e amigos.

MANTENHA SUA SENHA PROTEGIDA

Somente você deve ter acesso a sua senha. Nunca anote a senha em lugares onde outras pessoas podem ver, como anotar em papéis perto do computador ou onde passam outras pessoas. Não deixe que as pessoas vejam você digitar sua senha e nunca forneça sua senha para ninguém. Uma pessoa com acesso a sua senha pode causar problemas graves nas suas contas e que dificilmente poderá ser provado que não foi você.

Caso deseje escrever a senha em um papel para não esquecer, guarde esse papel em um lugar que somente você tenha acesso. Deixe sua senha bem escondida.

Realização
CONEXÃO POVOS da FLORESTA
cgi.br nic.br cgi.br

Apoio
UK Government

Se utilizar um computador ou celular de outra pessoa para acessar alguma conta pessoal, não salve a senha em dispositivos de terceiros. Mesmo sendo o celular de uma pessoa de confiança, sua senha pode ficar exposta e colocar suas contas em risco.

Faça uso de autenticação em dois fatores, ou seja, uma confirmação extra além da senha. Esse recurso exige, além da senha, um outro recurso para a autenticação. Esse recurso pode ser uma mensagem SMS, Whatsapp ou até mesmo ligação telefônica (esse recurso apenas envia um código para autenticação para confirmar sua identidade e nunca vai pedir para enviar a senha por e-mail ou aplicativo). Também existe a possibilidade de utilizar um aplicativo de autenticação. Para usuários de Android, tudo isso pode ser configurado na parte de segurança da sua conta.

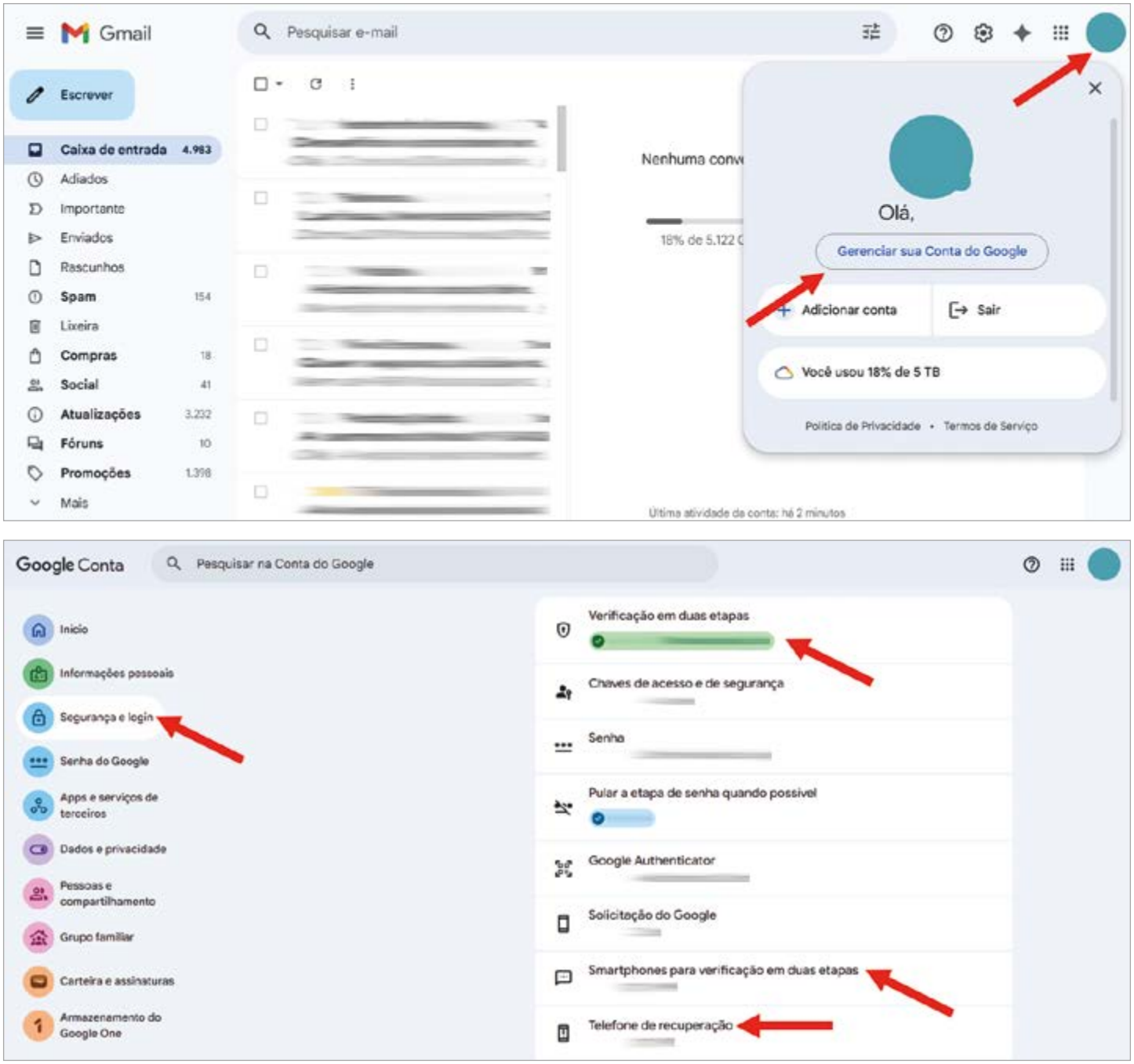


Figura 8: Elaboração própria

Os dois recursos têm vantagens e desvantagens: Receber uma mensagem por SMS ou Whatsapp é o recurso mais simples, mas menos seguro caso o celular seja furtado (já que o número do celular está nas mãos de quem furtou). Já o software de autenticação tem o uso um pouco mais complexo mas é mais seguro, já que gera códigos aleatórios para o acesso às contas.

QUANDO ALTERAR SUA SENHA?

Os vazamentos de listas de senhas costumam acontecer com uma certa frequência e nesses casos algumas senhas utilizadas podem ter sido compartilhadas. Por isso, o ideal é alterar a senha com alguma frequência. Essa frequência fica a critério de cada um, mas o ideal é não deixar a mesma senha por muito tempo.

Caso desconfie que sua senha foi descoberta, a recomendação é trocá-la imediatamente.

Realização

CONEXÃO POVOS da FLORESTA

cgi.br nic.br cgi.br

Apoio

UK Government

CONFIGURAÇÕES PARA AUMENTAR A SEGURANÇA

MANTENHA O SISTEMA OPERACIONAL E APLICATIVOS ATUALIZADOS

Softwares desatualizados podem ter brechas que abrem portas para códigos maliciosos. Verifique sempre se o sistema operacional e os aplicativos estão atualizados. Para verificar as atualizações de sistema operacional no Android, acesse o aplicativo de "configurações" e procure por "atualização de software".

Para atualizar os aplicativos, abra o app da Google Play Store e toque no seu ícone de usuário no topo da tela e selecione "gerenciar apps e dispositivos". Existe uma opção para atualizar todos os aplicativos desatualizados.

Lembre-se de sempre baixar aplicativos das lojas oficiais. Não baixe aplicativos de *link*s em *site*s ou recebidos por redes sociais.

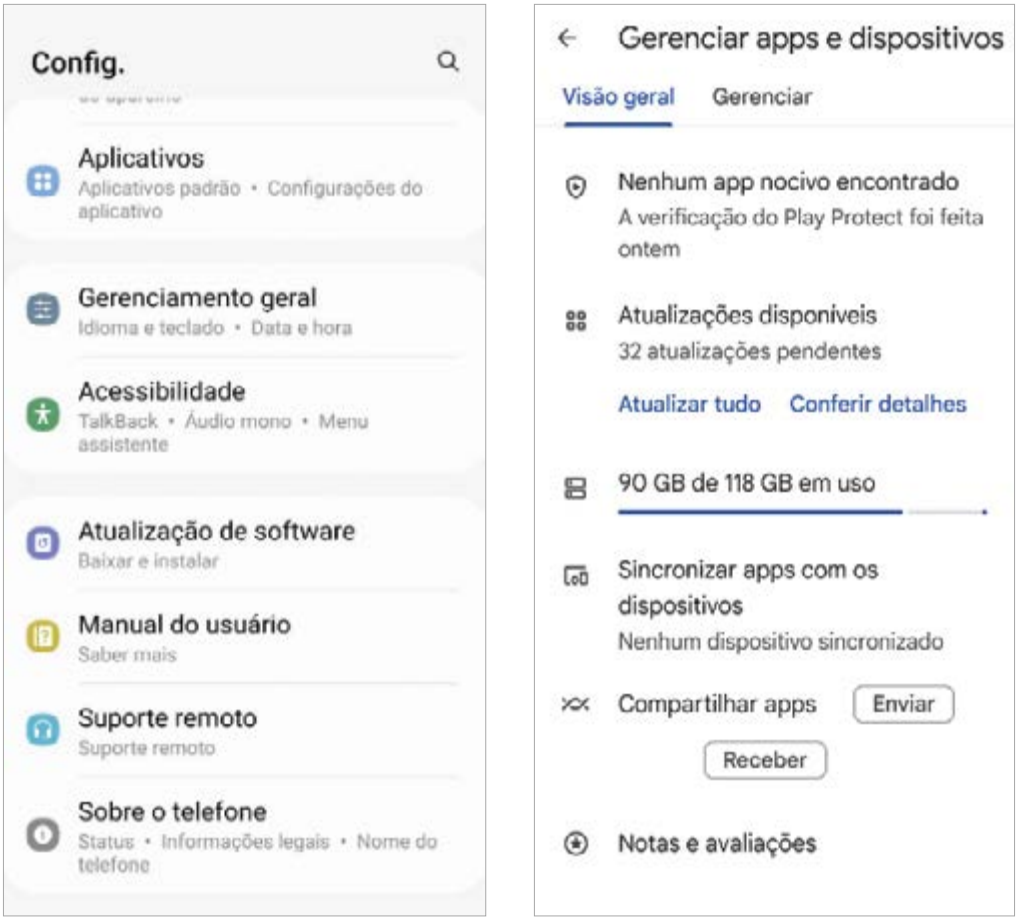


Figura 9: Elaboração própria

Situação real: o aparelho fica meses sem atualizar porque "gasta Internet demais".

Boa prática: atualizar quando estiver em Wi-Fi estável; priorizar atualizações de segurança.

Se não fizer: aumenta chance de golpes e invasões usando falhas antigas

Realização

Apoio

BLOQUEIE A TELA DE INÍCIO

O bloqueio da tela de início evita que o celular fique desbloqueado o tempo todo, permitindo que qualquer um o acesse se encontrá-lo aberto. Configure um tempo curto de inatividade para exigir uma senha, padrão ou reconhecimento facial. Esse recurso pode ser acessado no aplicativo "configurações" no item "tela de bloqueio".

FAÇA *BACKUP* DOS DADOS IMPORTANTES

Não deixe as informações importantes somente no seu celular. Mantenha cópias salvas na Internet ou em outros tipos de armazenamento como pen-drives ou HD externos. Assim, se teu celular foi furtado você não perde documentos importantes.

Realização

CONEXÃO POVOS da FLORESTA

cgi.br nic.br cgi.br

Apoio

UK Government

AUMENTAR A SEGURANÇA DO CELULAR

PROTEJA O CHIP DO CELULAR COM SENHA

O chip físico do seu celular possui dois códigos: O PIN e PUK. O PIN pode ser utilizado para bloquear o celular caso alguém retire o chip do seu dispositivo. Esse bloqueio vai exigir o número do PIN quando o novo celular for ligado com o seu chip.

Para ativar esse recurso abra o aplicativo de "configurações" e procure por "bloqueio SIM". O sistema vai pedir o número do PIN e depois permite sua alteração.

IMPORTANTE: Você precisa saber o seu número PIN (costuma estar marcado no cartão que vem com o chip). Caso não saiba, entre em contato com a operadora. Errar o PIN 3 vezes vai exigir outro código (PUK).

ANOTE O IMEI DO CELULAR EM LUGAR SEGURO

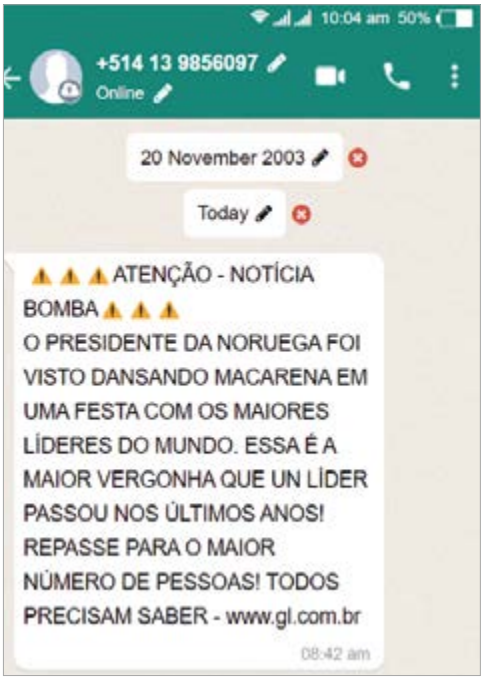
O código IMEI é um número exclusivo de cada celular. É muito importante anotar esse número pois em caso de furto você precisará desse número para bloquear o celular. Esse número está na nota fiscal e na caixa do dispositivo, mas caso não tenha mais esse documento ou caixa, basta abrir o discador do seu celular e digitar *#06# e o código será exibido na tela. Anote e guarde em um lugar seguro.

CADASTRE SEU CELULAR NO SISTEMA "CELULAR SEGURO"

O Ministério da Justiça lançou em 2024 o sistema Celular Seguro, que permite o bloqueio a distância do dispositivo e dos aplicativos instalados nele. Você pode acessar o sistema com sua conta GOV.br pelo endereço https://celularseguro.mj.gov.br/.

Para cadastrar o celular você precisa inserir alguns dados como o número do celular e o código IMEI.

IMPORTANTE: não faça um bloqueio teste para validar se a plataforma funciona, diversas pessoas bloquearam o celular de forma irreversível testando o aplicativo.



O QUE FAZER EM CASO DE FURTO DE CELULAR

Caso seu celular esteja cadastrado no sistema "Celular Seguro", em caso de furto do seu celular, o primeiro passo é bloquear o aparelho a distância por esse serviço. Entre em um computador ou outro dispositivo para fazer o bloqueio.

Cuidado, pois esse bloqueio pode ser irreversível.

Realização

CONEXÃO POVOS da FLORESTA

ceweb.br nic.br cgi.br

Apoio

UK Government

Em seguida, pegue o código IMEI e faça um boletim de ocorrência. Ligue também para a operadora para o bloqueio do chip e para os bancos para o bloqueio das contas. Eles devem pedir o número do boletim de ocorrência. Caso tenha feito o procedimento pelo *site* "Celular Seguro" eles já podem ter sido bloqueados, mas é recomendável ligar para as instituições e confirmar.

Troque todas as suas senhas, desde as senhas de e-mail e redes sociais até as de banco e aplicativos instalados no seu celular.

Você também pode apagar todas as informações do dispositivo a distância com um recurso do Google chamado "Encontre o meu dispositivo". Caso o celular ainda esteja conectado a Internet você pode apagar todos os dados a distância por este recurso. Cuidado, pois essa ação é irreversível.

CUIDADOS COM NOTÍCIAS FALSAS *(FAKE NEWS)*

Esse tipo de conteúdo é uma informação falsa criada por terceiros que é transmitida ou publicada como notícia, motivada por razões políticas ou para fins fraudulentos. Elas possuem algumas características comuns:

- Chamadas alarmistas "Atenção" e "Notícia bomba"
- Poucos detalhes como "onde foi?" "quando?"
- Costumam ter erros de português
- Costuma pedir para compartilhar a mensagem

O que fazer quando receber uma notícia falsa?

- Pesquise trechos da mensagem no Google
- Verifique a fonte da notícia
- Verifique se aparece em grandes canais de notícia
- Recorra a agências de checagem
- Não repasse a mensagem
- Denuncie

Situação real: áudios com mensagens alarmistas, como "vacina faz mal", "há perigo na região" ou "o benefício vai acabar hoje".

Boa prática: verifique as informações em fontes confiáveis, como agências de checagem; pesquise trechos da mensagem no Google e nunca compartilhe com outras pessoas sem ter certeza de que a informação é verdadeira.

Se não fizer: pode causar pânico, espalhar desinformação, levar a decisões prejudiciais (como na saúde), gerar conflitos e provocar diferentes tipos de prejuízo — morais, financeiros e materiais.

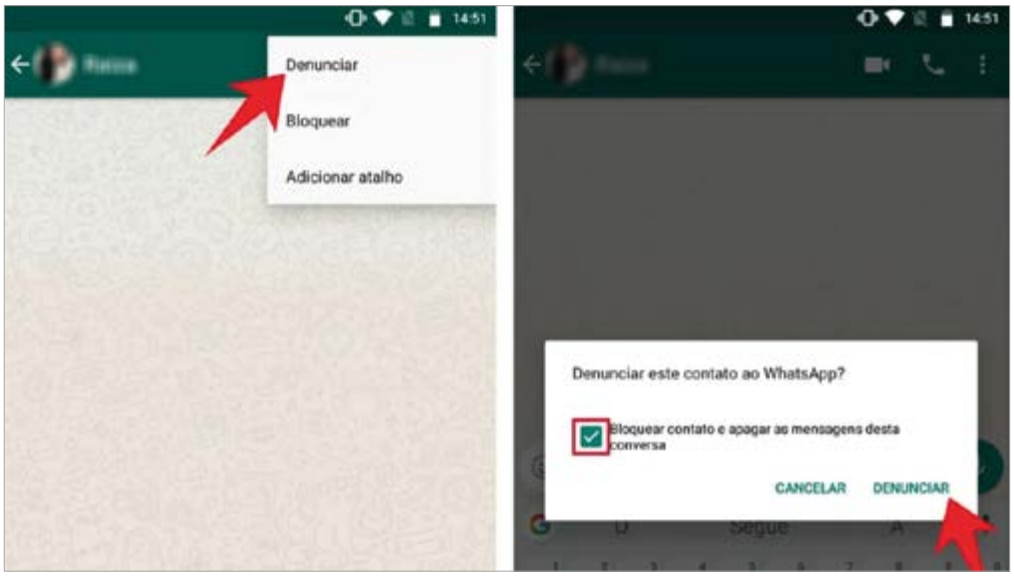
Realização
Conexão Povos da Floresta
cgi.br nic.br cgi.br
Apoio
UK Government

Agências de checagem são instituições ou grupos que pesquisam notícias falsas e publicam informações para saber se ela é verdadeira ou não. Se tem alguma dúvida, procure no Google pelas agências AFP Checamos, Agência Lupa, Aos Fatos, Boatos, Comprova, E-farsas, Estadão Verifica, Fato ou Fake, UOL confere dentre outros.

Com o avanço da Inteligência Artificial Generativa, temos visto o surgimento das Deep Fakes, que criam vídeos, áudios e imagens que parecem extremamente reais, mas que não são. Assim, mesmo que notícias ou informações cheguem em formato de vídeo, desconfie – especialmente se tiver caráter político, ou quiser prejudicar a reputação de alguém. Busque sempre por fontes confiáveis!

COMO DENUNCIAR NOTÍCIAS FALSAS OU FRAUDULENTAS

No seu aplicativo de mensagens ou rede social, procure na tela da mensagem os ícones como três pontinhos ou outras ações. Na mensagem do whatsapp e no instagram ela aparece no topo esquerdo da mensagem. Procure por "denunciar" nesse menu e faça a denúncia. Ela é feita de forma anônima, então a pessoa que enviou ou publicou não saberá que você foi o denunciante.



Realização
Apoio

#INTERNETCOMRESPONSA

Agora que entendemos como funciona a Internet e como navegar na Web com segurança, é muito importante que seja entendido também como podemos fazer esse uso com consciência, ética e respeito. Apesar da sensação de anonimato, existe a possibilidade de rastreamento e, em casos mais graves, até mesmo punições previstas em lei.

> *"A Internet é um território de oportunidades, oferece acesso a informações importantes, os aproxima de amigos e parente, permite conhecer lugares que ainda não pisaram, porém, se eles não utilizarem a Internet com a mesma consciência e responsabilidade, com que agem na vida real, podem (se já não aconteceu) ser vítimas de ciladas e ter muitos prejuízos materiais, físicos e morais."*
> *Fonte: Internet Segura. (2023).*

CUIDADO COM O QUE POSTA NAS SUAS REDES SOCIAIS

Evite postar informações pessoais nas redes sociais, não revele hábitos ou compromissos frequentes e tenha cuidado ao divulgar imagens dos seus amigos e parentes. Limite o acesso de pessoas que você não conhece a aquilo que você posta, bloqueando ou restringindo o acesso de pessoas desconhecidas. Pessoas mal intencionadas podem utilizar o conteúdo que você posta para praticar atividades maliciosas contra você, seus parentes e seus amigos.

NÃO SE PASSE POR OUTRA PESSOA NA INTERNET

Não crie perfis falsos para prejudicar pessoas, evite compartilhar conteúdo que possa ser prejudicial a terceiros e pense antes de fazer comentários que afetem a imagem de alguém. Evite divulgar informações falsas ou humilhantes. Lembre-se de que o que parece uma brincadeira inocente pode ser um crime com punição prevista em Lei.

CUIDADOS AO CONVERSAR PESSOAS *ONLINE*

Não use *webcam* com desconhecidos, evite gravar ou permitir que gravem vídeos e fotos íntimas suas. Evite marcar encontros com desconhecidos pela Internet. Salve em outro lugar ou delete fotos e arquivos pessoais ao consertar dispositivos.

Tenha cuidado ao se associar a grupos *online*. Certos grupos podem transmitir discurso de ódio, fotos e vídeos de atividades criminosas ou ilícitas. Caso encontre algo assim em grupos que participe, denuncie.

CYBERBULLYING E DISCURSO DE ÓDIO

Cyberbullying (que, por sinal, é o mesmo que *bullying*) é algo muito grave e caracteriza-se por intimidar, pela Internet, outra pessoa, com insultos e apelidos pejorativos, colocando-a em isolamento, excluindo-a ou diferenciando-a dos outros.

Mas, talvez o que você não saiba é que o *bullying* é um crime previsto na Lei 14.811 de 2024, acrescentou o artigo 146-A ao Código Penal.

Realização
CONEXÃO POVOS da FLORESTA
ceweb.br nic.br cgi.br
Apoio
UK Government

Não pratique nem estimule o *bullying* em grupos, redes sociais ou comunicadores instantâneos. Caso presencie situações de *bullying*, denuncie na plataforma que está utilizando.

INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial (IA) é um tipo de tecnologia feita para simular algumas capacidades humanas, como entender perguntas, dar respostas, reconhecer imagens ou até conversar com você. Ferramentas como ChatGPT, DeepSeek ou Gemini são um tipo de IA chamada Modelo de Linguagem, criada para conversar, explicar assuntos e ajudar em várias tarefas do dia a dia.

Essas ferramentas funcionam porque foram treinadas com uma grande quantidade de conteúdos: notícias, livros, *site*s públicos e outros conteúdos. A partir disso, a IA aprende padrões e tenta prever a melhor resposta com base nas palavras que você digita.

Mas é importante ter alguns cuidados. A IA trabalha com probabilidades, então não é possível ter certeza que a resposta da IA está sempre correta. Às vezes pode inventar informações ou apresentar dados desatualizados. Por isso, sempre que possível, é bom conferir em fontes confiáveis se a resposta está correta.

A IA pode ser muito útil, mas a gente precisa usá-la com olhar crítico e sem confiar 100% em tudo que ela fala. Pense nela como uma ferramenta de apoio, não como uma ferramenta que sabe de tudo.

ENCERRAMENTO

Cuidados com o nosso patrimônio *online* nunca é demais. Lembre-se que o que acontece na Internet pode interferir na sua vida fora dela. Mantendo boas práticas de uso da Web, segurança e privacidade podemos tornar o ambiente *online* mais saudável e seguro para todos.

Este guia é um compilado de uma série de materiais sobre boas práticas de uso da Web, segurança e privacidade produzidos pelo NIC.br. Você pode encontrar mais materiais sobre esses temas nos *link*s a seguir:

Guia Internet Com Responsa: https://Internetsegura.br/pdf/Internet_com_responsa.pdf

Fascículos sobre privacidade, proteção e compartilhamento de dados, banco via Internet, backup e outros assuntos relacionados a segurança digital: https://cartilha.cert.br/fasciculos/

Realização

CONEXÃO POVOS da FLORESTA

cgi.br nic.br cgi.br

Apoio

UK Government