dialogando
vivo

Segurança on-line para crianças e adolescentes

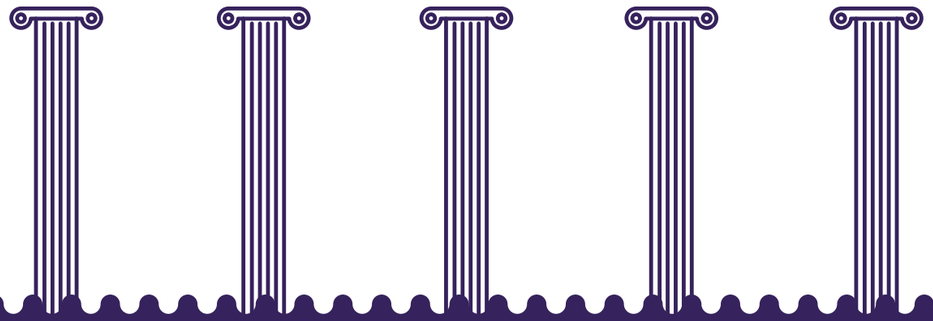
Índice

O Dialogando

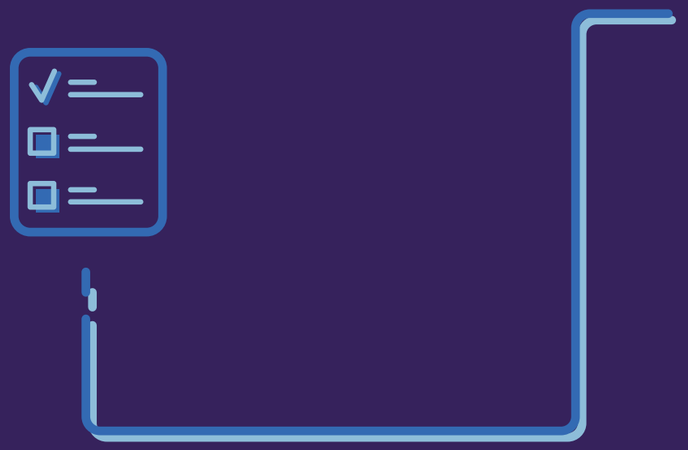
Desde 2016, o portal Dialogando tem como objetivo promover a discussão sobre o uso consciente da tecnologia. Com o respaldo da Vivo, o portal ocupa um espaço que nenhuma empresa de telecomunicações conquistou, e o faz por meio da abordagem educativa de temas relacionados ao uso consciente da internet e seus impactos na vida das pessoas e da sociedade.

Presente em 12 países, com versões em português e espanhol, o Dialogando aborda a tecnologia em 5 pilares diferentes: Sustentabilidade, Educação, Inovação, Segurança e Comportamento.

Sustentabilidade **Educação** **Inovação** **Segurança** **Comportamento**



A cartilha



A internet está presente no cotidiano de grande parte de crianças e adolescentes. Hoje, é possível fazer pesquisas, acessar as redes sociais, encontrar amigos, se informar, jogar e até mesmo estudar com ela — basta ter acesso à rede por meio de um computador, *tablet* ou *smartphone*.

Entretanto, para que eles possam aproveitar uma navegação segura, é preciso tomar alguns cuidados. Esta cartilha foi elaborada para ajudar famílias, cuidadores e responsáveis a garantir a segurança de crianças e adolescentes no ambiente digital. Queremos te inspirar a iniciar ou ampliar o diálogo sobre esses temas, buscando uma internet positiva e segura para todos!

PRIVACIDADE ON-LINE, APLICATIVOS E TERMOS DE USO

Já parou para pensar na quantidade de informações que compartilhamos na hora de fazer um cadastro em um site? Nas redes sociais, são fotos, check-ins, dentre outros dados que, há algumas décadas, jamais compartilharíamos com estranhos.

Sempre que um aplicativo é instalado surge um termo de uso com uma lista de permissões para aceitar. O app pode pedir permissão para envio de notificações, acessar galeria de fotos, câmera, agenda, lista de contatos, localização, microfones e sensores.

A maior parte dos aplicativos funciona normalmente, mesmo quando não consentidas algumas permissões. Por isso, não é recomendado aceitar o que parecer um excesso. Se determinada permissão for realmente necessária, o sistema operacional do aparelho vai avisar que sua retirada pode prejudicar o funcionamento do app.

ATENÇÃO: apps também possuem classificação indicativa de faixa etária. Confira o quadro com a informação da idade na loja oficial.

Avalie bem a necessidade de um app ter acesso aos dados pessoais

Ao examinar com calma as permissões de aplicativos, é possível avaliar melhor se vale a pena mesmo instalar. Principalmente nos aplicativos gratuitos, como o Facebook, há a condição de fornecer alguns dados básicos ou mesmo permitir o acesso a publicações da sua conta, o que pode não ser o ideal.

Desconfie de acessos que não tenham relação com as funções do aplicativo

Para proteger os dados, fique atento se o que está sendo autorizado tem a ver com a função ou serviço oferecido, como uma liberação de acesso à câmera para aplicativos que não utilizem imagens. Isso pode ser um indício de aplicativos mal-intencionados. Na dúvida, não instale!

Faça *downloads* somente em lojas e sites confiáveis

Não confie em fontes ou desenvolvedores anônimos quando for realizar um *download* na Play Store (Android) ou Apple Store (iOS). O mesmo vale para os sites: confie somente em lojas oficiais!

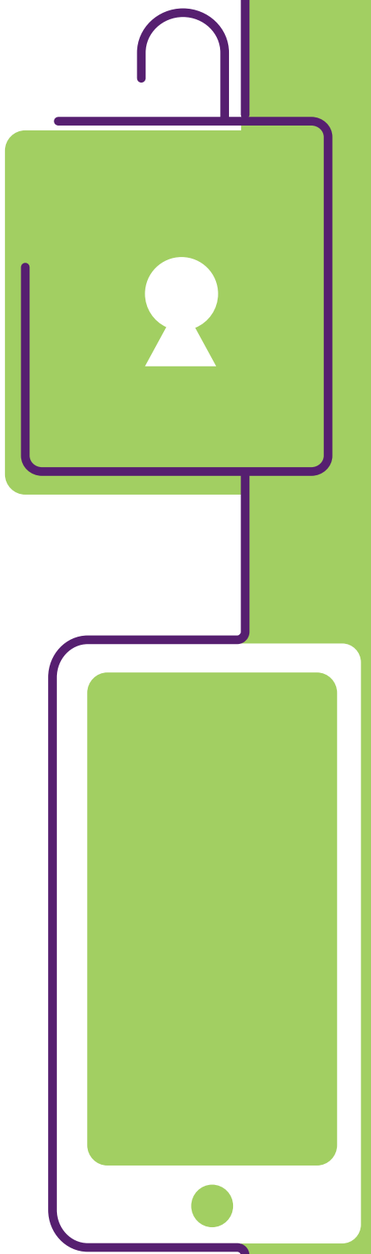
SENHAS E AUTENTICAÇÃO EM DOIS FATORES

O primeiro passo para garantir a proteção durante o acesso à internet é, ao se cadastrar em sites e redes sociais, criar uma senha complexa, que não possa ser descoberta facilmente, e, sempre que disponível, dentro dos padrões de segurança recomendados pelo site que você estiver acessando. Algumas dicas simples:

- Senhas fortes possuem combinações de letras maiúsculas, minúsculas, números e caracteres especiais.
- Não é recomendado usar uma senha que já foi usada anteriormente.
- Informações como datas de nascimento e números de documentos não devem ser utilizadas.

A autenticação em dois fatores é um mecanismo de segurança que oferece uma segunda camada de proteção — sendo a primeira a senha e o login do usuário para acessar um site ou rede social.

Criado para proteger os usuários que utilizam serviços on-line, esse sistema começou a ser muito utilizado por ser caracterizado como uma medida contra invasões, roubos e tentativas de fraude on-line. A autenticação em dois fatores pode ser feita por meio de um token, envio de SMS com o código do *token* ou envio de e-mail para confirmação de acesso.



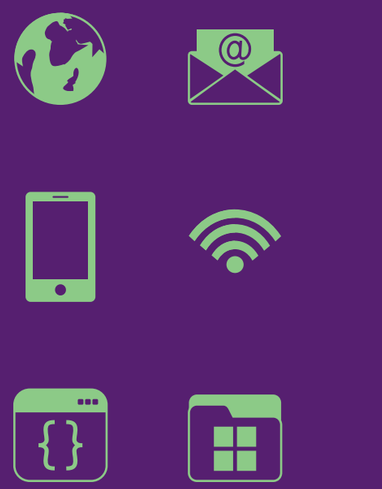
SMARTPHONES E COMPUTADORES

Para proteger dispositivos móveis como *smartphones* e *tablets*, confira estas dicas:

- Antes de instalar aplicativos de redes sociais e jogos, é recomendado instalar um antivírus ou *antimalware*.
- É preciso ter cuidado ao instalar aplicativos de desenvolvedores "anônimos", que não sejam de empresas especializadas e verificadas.
- É importante estar atento aos aplicativos que solicitam informações baseadas em geolocalização.
- Redes Wi-Fi públicas devem ser utilizadas com cautela.
- As interfaces de comunicação, como *Wi-Fi* e *bluetooth*, devem permanecer desligadas quando não estiverem sendo utilizadas.

Para proteger computadores de ataques virtuais, existem algumas dicas simples:

- Antivírus e o *firewall* devem estar atualizados.
- *Downloads* em sites não confiáveis devem ser evitados.
- É necessário sempre realizar o logout de sites e redes sociais antes de fechar o navegador web.
- O histórico de navegação de sites visitados deve ser apagado constantemente.
- A utilização de *cookies* de sites desconhecidos não deve ser permitida (os *cookies* guardam informações e preferências ao acessar os sites posteriormente).



APLICATIVOS DE MENSAGEM

Os aplicativos de mensagens instantâneas estão, atualmente, entre os mais baixados e utilizados. Nessa troca constante de informações, renova-se a importância da proteção dos seus dados. Por isso, o vazamento e o roubo de informações estão entre os assuntos mais debatidos e noticiados, trazendo à tona tópicos relevantes sobre privacidade on-line e segurança digital.

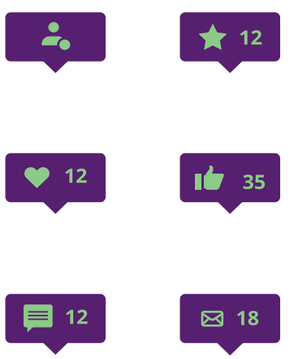
Alguns hábitos e cuidados evitam e previnem invasões de criminosos cibernéticos:

- Senha de acesso ou a digital para bloquear acesso ao aplicativo, sempre que disponível. As senhas devem ser fortes, com números, símbolos, letras e, em alguns casos, a sensibilidade entre maiúsculas e minúsculas, que oferece maior dificuldade no acesso.
- Os aplicativos devem estar sempre atualizados, para ficar com o máximo de proteção contra falhas.
- A autenticação em dois fatores deve estar sempre habilitada.

O Telegram oferece bloqueio do aplicativo por senha e a criação de conversas que se autodestroem após certo tempo, chamadas de “chats secretos”.

O WhatsApp usa criptografia em todo conteúdo (proteção dos dados), além de oferecer a opção de autenticação em duas etapas.

O Messenger possui como segurança uma senha *master* e um PIN numérico. Ainda há a possibilidade de configurar uma resposta de segurança em caso de esquecimento.



REDES SOCIAIS

As redes sociais podem ser uma fonte de entretenimento, estudos e desenvolvimento, se usadas com moderação e segurança. Estar conectado é cada vez mais comum. Porém, é necessário saber lidar com os possíveis riscos de contato com pessoas mal-intencionadas, conteúdos impróprios e exposição excessiva.

Algumas medidas e ferramentas para o uso das redes sociais de forma mais positiva e segura para todos são:

- A importância de educar sobre o uso consciente e moderado das redes e estipular, por exemplo, o tempo de uso limite diário.
- Fazer a revisão das configurações de segurança e privacidade para controle da experiência.
- Solicitações de pessoas desconhecidas devem ser rejeitadas e bloqueadas.
- Realizar denúncias quando necessário – cada plataforma possui uma central de atendimento para tirar dúvidas ou tomar medidas.

CYBERBULLYING

Por definição, o *cyberbullying* se caracteriza pela prática que envolve o uso de tecnologias de informação e comunicação para dar apoio a comportamentos deliberados, repetidos e hostis cometidos por um indivíduo ou grupo com a intenção de prejudicar o outro.

Algumas agressões podem ser consideradas crimes quando praticadas entre adultos, em geral, crimes contra honra segundo o código penal, a exemplo de:

- **Calúnia:** alguém que imputa a outrem falsamente fato definido como crime;
- **Difamação:** alguém que imputa a outrem fato ofensivo à sua reputação;
- **Injúria:** alguém que ofende a dignidade ou o decoro de outrem.

A questão é tão grave e tem assumido dimensões tão grandes que o governo brasileiro instituiu, em 2015, uma lei que cria o Programa de Combate à Intimidação Sistemática em todo o território nacional. A SaferNet Brasil – ONG referência na proteção de direitos humanos na Internet – recomenda algumas ações para combater o *cyberbullying*:

- Discutir ética nas relações de amizade;
- Fomentar ambientes mais inclusivos;
- Importância de a escola oferecer espaços para que as vítimas possam pedir ajuda;
- Campanhas de sensibilização;
- Incentivar a participação dos adolescentes na busca de soluções. Eles devem ser atores no debate;
- Reconhecer iniciativas e boas práticas sobre o tema e premiar quem faz o bem.

EXPOSIÇÃO DE IMAGENS ÍNTIMAS

O termo *nudes* define as imagens íntimas que circulam on-line. Alguns adolescentes trocam esse tipo de conteúdo em seus relacionamentos, abrindo brechas para situações de violação da intimidade, exposição sem autorização ou até aliciamento sexual.

*Pelo artigo 241 do Estatuto da Criança e do Adolescente, é crime produzir, distribuir, armazenar ou trocar conteúdo que envolva crianças ou adolescentes em atividades sexuais explícitas, reais ou simuladas, ou exibição dos seus órgãos genitais para fins primordialmente sexuais.

- Jamais compartilhar imagens íntimas por impulso ou pressão.;
- Em caso de dúvidas ou suspeitas, é melhor não realizar o envio;
- Se houver ameaça, é importante pedir ajuda, bloquear o usuário e denunciar imediatamente;
- Compartilhar *nudes* dos outros sem consentimento é crime!
- Pais, mães, educadores e responsáveis precisam acolher e ajudar, antes de julgar. Isso ajuda a quebrar o silêncio para prevenir casos de abuso.

TODOS POR UMA INTERNET MAIS SEGURA

É importante ficar atento e levar todas as dicas e informações preventivas para o dia a dia no ambiente digital. Qualquer violação dos direitos de crianças e adolescentes deve ser denunciada aos órgãos competentes.

Para realizar denúncias on-line, a SaferNet disponibiliza o canal https://new.safernet.org.br/denuncie, que recebe denúncias de diversos tipos de crimes contra os direitos humanos: racismo, intolerância religiosa, violência sexual contra crianças, homofobia, misoginia, entre outros.

Além das denúncias, a plataforma oferece ainda um Canal de Ajuda para orientação sobre casos de *cyberbullying*, *sexting* e extorsão, exposição de imagens íntimas, uso saudável da tecnologia e outros temas de cidadania digital.

Com informação e o uso consciente da tecnologia, a internet pode se tornar um lugar seguro para todos!

REFERÊNCIAS

CERT.BR
cartilha.cert.br

CARTILHA HELPLINE SAFERNET
new.safernet.org.br/content/cartilha-helpline

CETIC.BR - TIC Educação 2018
cetic.br/pesquisa/educacao/indicadores

PORTAL DIALOGANDO
dialogando.com.br

DIA DA INTERNET SEGURA NO BRASIL
http://www.diadainternetsegura.org.br

PORTAL INTERNETSEGURA.BR
internetsegura.br

RELATÓRIO WE ARE SOCIAL E HOOTSUITE SOBRE REDES SOCIAIS E CONSUMO DE INTERNET MUNDIAL
https://wearesocial.com/global-digital-report-2019

SAFERNET
new.safernet.org.br