

SaferDic@s



Brincar, estudar e...
Navegar com segurança na Internet!

Copyright © 2013 SaferNet Brasil

Esta obra é licenciada pela Creative Commons By-NC-SA
<http://creativecommons.org/licenses/by-nc-sa/3.0/br>

A reprodução do todo ou parte deste documento é permitida somente para uso não comercial, atribuição da fonte e compartilhamento pela mesma licença 3.0 Brasil.

Título original: SaferDicas: Brincar, estudar e ... Navegar com segurança na Internet

Conteúdo disponível também no *site* da Safernet Brasil www.safernet.org.br/cartilha

ISBN: 978-85-65151-00-9

Distribuição Gratuita.

1ª edição : 2008

2ª edição : 2009

3ª edição : 2010

4ª edição : 2011

5ª edição : 2013

Grupo de Trabalho da Equipe SaferNet para a realização da cartilha:

Thiago Tavares - Diretor Presidente

Rodrigo Nejm - Diretor de Prevenção

Caio SBA - Coordenação de TI

Melissa Wen - Suporte TI

Donminique Azevedo - Assessoria de Comunicação

Leila Grave - Psicóloga

Bianca Orrico - Psicóloga

Capa, ilustrações e *design*: Bruno Aziz

Normalização bibliográfica : Neubler Nilo Ribeiro da Cunha (CRB-5/1578)

Impresso no Brasil com o apoio financeiro da Petrobras - Programa Desenvolvimento e Cidadania

Dados Internacionais de Catalogação na Publicação

S128 Saferdicas: Brincar, estudar e... Navegar com segurança na Internet!--.Salvador: SaferNet Brasil, 2012.
48p. :il.

1. Internet . 2. Segurança na Internet. 3.Segurança Virtual

CDD - 004.6

Apresentação

A Cartilha SaferDic@s foi elaborada pela equipe da SaferNet Brasil com o propósito de contribuir para a promoção do uso ético, responsável e seguro da Internet no Brasil. Com uma linguagem simples, ilustrações inéditas e diagramação lúdica, a Cartilha pretende atingir públicos de diferentes faixas etárias, classes sociais e níveis educacionais.

A nova impressão de 15 mil exemplares desta Cartilha é uma das ações educativas previstas no Projeto: "Central Nacional de Denúncias de Crimes Cibernéticos", que conta com patrocínio da Petrobras através do Programa Desenvolvimento e Cidadania.

O conteúdo foi desenvolvido a partir de pesquisas sobre conceitos, termos e novas linguagens usadas na Internet e no mundo digital. O objetivo deste material pedagógico é estimular os brasileiros, principalmente crianças e adolescentes, a aproveitar todo o potencial da rede, sem esquecer de adotar os cuidados necessários neste novo espaço público, seguindo as dicas de segurança, ética e cidadania.

Cada vez mais cedo, a Internet passa a ocupar um lugar privilegiado nas nossas vidas e precisamos saber como desfrutar ao máximo das inúmeras qualidades disponíveis. Orientação, diálogo e conscientização continuam sendo as melhores tecnologias para evitar os perigos e violações de direitos na Internet.

Como contribuição para a conscientização dos internautas, disponibilizamos para toda a sociedade uma versão *on-line* da Cartilha, com possibilidade de *download* para quem quiser imprimir, distribuir ou guardar como referência. Basta acessar no portal www.safernet.org.br/cartilha

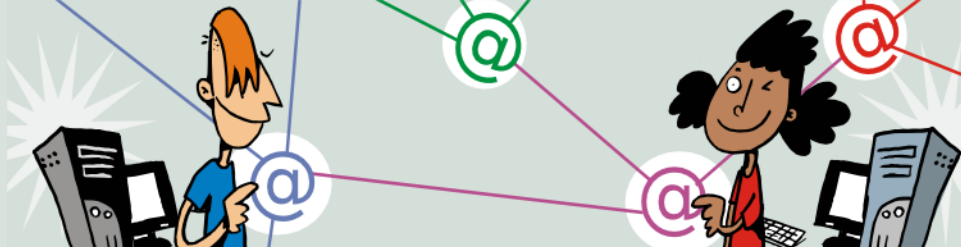
Desejamos que educadores, estudantes, pesquisadores, pais e toda a sociedade brasileira tenham acesso e divulguem o conteúdo da Cartilha, especialmente elaborada para potencializar o uso saudável e responsável da Internet.

Forte abraço,

SaferNet Brasil

Sumário

Internet	05
Navegadores ou <i>Browsers</i>	06
<i>Sites</i> de Busca	07
LAN <i>house</i> e Infocentro	08
<i>E-mail</i>	09
<i>Chat</i> e Salas de Bate Papo	10
<i>Webcam</i>	11
<i>Sites</i> de Redes Sociais	12
<i>Blogs, Fotologs e Microblogs</i>	13
Redes P2P	14
Jogos <i>On-Line</i>	15
Privacidade	16
Uso excessivo	17
Cibercrime - Crime Digital	18
<i>Cyberbullying</i>	19
<i>Sexting</i>	20
Aliciamento Sexual Infantil <i>On-Line</i>	21
Conteúdos Impróprios	22
Roubo de Dados	23
Justiceiros Virtuais	24
Helpline	25
Denuncie	26
Conheça Também...	27
Safernet	28
<i>Software</i> Livre	29



Internet

Rede de milhões de computadores de todo o mundo interligados por linhas telefônicas, fibra ótica e satélites. Além de ligar redes de computadores, conecta milhões de pessoas que formam suas redes de relacionamento e navegam pelas informações disponíveis no espaço virtual, também chamado de Ciberespaço. Tem sido cada vez mais comum o uso do celular para navegar na Internet.



Aproveite!

- Acesso e troca de diferentes tipos de materiais como imagens, sons, vídeos e textos;
- Permite a comunicação e amizade entre pessoas de qualquer lugar do mundo;
- Rica fonte para estudos, pesquisas, trabalho e diversão;
- Supera limites de tempo e espaço, criando um novo espaço público: o ciberespaço.



Cuidado!

- Pode ser prejudicial se usada sem limites ou quando substitui todas as outras atividades de lazer;
- Como todo espaço público, pode ser acessada por pessoas mal intencionadas;
- A Internet não é "terra sem lei". Apesar da sensação de anonimato, quem pratica crime por meio dela pode ser identificado e punido;
- Não podemos confiar em todas as informações, nem em todas as pessoas conectadas;
- Proibir não educa nem previne. Dialogue e busque orientação.



Dicas para manter-se seguro

- Nunca divulgue senhas, nome completo, endereços, números de telefone ou fotos íntimas;
- Você distribuiu qualquer foto sua no mural da escola, no ônibus ou na praia? Por que então divulgar na Internet? Pense bem antes de publicar algo. Uma vez na rede, é quase impossível controlar o uso;
- Comunique-se com educação. Respeito deve valer em qualquer espaço e com qualquer pessoa, mesmo com aquelas que não conhecemos;
- Evite gravar as senhas e *login* no computador para não facilitar roubos;
- Cuidado ao baixar arquivos, eles podem conter vírus, materiais impróprios ou ser ilegais. Antivírus e filtros podem ajudar a proteger;
- Nunca aceite que *sites* instalem programas em seu computador e não faça *download* de algo que você não saiba exatamente o que é e de onde vem;
- Busque provedores e serviços que ofereçam recursos de segurança, que sejam éticos e responsáveis;
- Dialogue sempre com amigos, filhos e professores para se manter informado sobre segurança na Internet;
- Se precisar de ajuda para tirar suas dúvidas, acesse: www.canaldeajuda.org.br



Navegadores ou Browsers

Programas que permitem visualizar os conteúdos e "surfar" nas páginas na Internet. Os mais conhecidos são o Mozilla Firefox e o Internet Explorer.



Aproveite!

- Uso simples e dinâmico para navegar na Internet;
- Permitem ajustes para apagar senhas, filtrar e copiar páginas;
- Ajudam a guardar os endereços para voltar aos *sites* preferidos.



Cuidado!

- Geralmente não identificam sozinho páginas falsas ou ilegais. O usuário é quem define o que visitará. No programa, tudo pode ser visto;
- Cuidado com os *sites* ilegais e com conteúdos impróprios para crianças;
- O navegador não garante sozinho a segurança de informações pessoais, senhas e dados bancários.



Dicas para manter-se seguro

- Sempre leia com atenção as mensagens mostradas pelo navegador, pois elas podem ajudar a identificar um programa malicioso ou um *site* falso;
- Não autorize instalação de *software* de desconhecidos ou de *sites* estranhos;
- Use o bloqueio de *pop-up* em seu navegador;
- Quando digitar um endereço, confirme se o que está na tela é exatamente o que procurava;
- Atenção com transações financeiras via Internet. Quando as fizer, confira se aparece o desenho de um "cadeado fechado" no rodapé da página e se o endereço começa com "https", em vez de "http";
- Dê preferência aos navegadores de Internet livres que são mais seguros, a exemplo do Mozilla Firefox, Epiphany, Konqueror. Em caso de visualizar conteúdos suspeitos de violar os Direitos Humanos, denuncie em www.denunciar.org.br e bloqueie o endereço.



Sites de Busca

São páginas que oferecem o serviço de busca de conteúdos disponíveis em outros *sites* na Internet a partir de expressões ou palavras-chave. Em geral, os *sites* de busca são gratuitos e apontam outros endereços onde é possível encontrar o conteúdo buscado. Exemplo: Google, Bing, Yahoo...



Aproveite!

- Permitem pesquisas rápidas em quase todo conteúdo da Internet entre fotos, vídeos, textos, livros, músicas, imagens, programas etc;
- Os maiores são gratuitos e atualizados a todo instante;
- Facilitam achar o que queremos na imensidão do ciberespaço.



Cuidado!

- Podem apresentar conteúdos indesejados ou diferentes do procurado;
- Geram resultados de acordo com as palavras-chave, mesmo quando escritas de forma errada;
- Geralmente exibem o resultado da busca baseado na popularidade, e não na relevância;
- Mesmo os conteúdos ilegais podem ser encontrados nas buscas;
- Crianças podem facilmente encontrar conteúdos agressivos e impróprios.



Dicas para manter-se seguro

- Não confie em tudo o que vê ou lê, muitos conteúdos são falsos e mentirosos;
- Os *sites* de busca não substituem as bibliotecas, estimule a leitura. Na biblioteca, também pode ser legal navegar;
- Para evitar resultados muito amplos, coloque as palavras entre aspas (" ");
- Feche as páginas que não estão relacionadas ao assunto esperado para evitar constrangimento;
- Use o serviço de pesquisa segura (*Safe Search*) dos buscadores.
- Procure em preferências e ative a filtragem de páginas com conteúdo sexual explícito, impedindo que elas apareçam nos resultados da pesquisa;
- Em caso de visualizar conteúdos suspeitos de violar os Direitos Humanos, denuncie em www.denunciar.org.br



LAN house e Infocentro

São centros públicos de acesso à Internet com vários computadores em rede. Os Infocentros e Telecentros são espaços criados e apoiados pelos governos para ampliar o acesso gratuito à Internet no País. A diferença entre eles e as LAN houses (ou Cibercafés) é que as LAN houses são comerciais e cobram pelo acesso. No Brasil, em 2008, cerca de 48% dos internautas brasileiros acessaram a Internet por meio de uma LAN house. Entre os jovens internautas de 10 a 15 anos, este número sobe para 63%, segundo dados de pesquisa do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) de set/nov 2008.



Aproveite!

- Facilitam o acesso à Internet para quem não tem computador ou não dispõe de conexão com a Internet;
- Permitem o acesso à Internet para quem está longe de casa;
- Disponibilizam pontos de acesso nos bairros para estudar, jogar, conversar e pesquisar.



Cuidado!

- Algumas cidades e alguns estados exigem autorização para acesso de crianças desacompanhadas;
- Quando não há exigência de identificação ou cadastro, pode ser aproveitada para esconder pessoas mal intencionadas ou que praticam crimes pela Internet;
- O acesso sem orientação adequada pode colocar as crianças e adolescentes em risco;
- Nem sempre o ambiente é próprio para meninos e meninas, conheça os responsáveis pelo espaço.



Dicas para manter-se seguro

- Lembrem-se sempre de clicar em "sair" antes de fechar as páginas e os programas;
- Atenção para não deixar suas senhas gravadas;
- Use somente o tempo necessário para evitar desperdício de tempo e dinheiro;
- Não aceite ajuda de estranhos e chame sempre o responsável em caso de dúvida;
- Evite acessar bancos e fazer compras por LAN houses ou Infocentros, se precisar de ajuda para tirar suas dúvidas, acesse: www.canaldeaajuda.org.br



E-mail

Serviço de troca de mensagem e “cartas” oferecido pela Internet. Permite enviar e receber textos, imagens, apresentações e quase todo tipo de informação em formato digital. A comunicação não é simultânea, você envia e recebe as mensagens por meio de uma caixa postal que fica em um dos computadores interligados à Internet. Para conferir suas novas mensagens, é preciso entrar periodicamente em sua caixa postal na Internet. Os endereços de *e-mail* são sempre identificados com “@” entre os nomes. Exemplos: voce@safernet.com.br (acentos não são aceitos).



Aproveite!

- Muitos são gratuitos e permitem que todos tenham sua própria “caixa postal” na Internet;
- Facilitam a troca de textos, fotos e vídeos entre as pessoas de todo o mundo;
- Agilizam a comunicação, pois as mensagens levam apenas alguns instantes para chegar ao destino com pouco custo, independentemente da distância.



Cuidado!

- Pode haver muitas informações falsas e golpes nas mensagens;
- Criminosos podem se aproximar para prejudicar, difamar e roubar;
- Crianças podem receber conteúdos impróprios e até serem aliciadas;
- Método mais utilizado para espalhar vírus;
- Atenção para aquelas propostas mirabolantes ou produtos milagrosos, pois geralmente estes são fraudes.



Dicas para manter-se seguro

- Você pode configurar sua conta para bloquear contatos indesejados;
- Evite senhas com informações óbvias (como nome, data de aniversário ou número de telefone). Misture sempre letras, números e outros caracteres.
- Não aceite nem abra *e-mail* de desconhecidos! Simplesmente apague sem ler;
- Procure saber a origem da informação e se o responsável é de confiança ou conhecido;
- Tenha muito cuidado com cartões virtuais. Não abra arquivos cujo nome possui “.exe” ao final;
- Evite mostrar seu endereço, número pessoal e outros detalhes. Seja genérico;
- Atualizar o antivírus e usar anti-Spam podem ajudar;
- Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por *e-mail*. Comunique-se por telefone com a instituição que supostamente enviou o *e-mail* e confira o assunto;
- Caso receba *Spam*, denuncie ao próprio serviço de *e-mail* e acesse: www.antispam.br/



Chat e Salas de Bate-Papo

Comunicação em tempo real que ocorre dentro dos *sites* de redes sociais, pelos celulares ou em salas temáticas *on-line*. Geralmente são abertas e todos os participantes podem ver e gravar as conversas. Cada vez mais estão usando também vídeos para ampliar os recursos da conversa.



Aproveite!

- Permitem conhecer e conversar "ao vivo" com pessoas de qualquer lugar do mundo;
- Facilitam o compartilhamento de ideias e a realização de debates pela Internet;
- Estimulam a participação em discussões sobre temáticas diversas;
- Podem contribuir com a socialização e desenvolver habilidades de comunicação.



Cuidado!

- As salas são espaços públicos abertos a qualquer um;
- É preciso ser educado e respeitar o outro mesmo em ambientes *on-line*;
- Existem salas de bate-papo que são impróprias para crianças. Cuidado com quem seus filhos conversam!
- Em ambientes *on-line*, pessoas podem fingir ser quem não são, por isso, tenha muito cuidado ao conversar com pessoas que você só conhece pela Internet;
- Os apelidos dificultam a identificação e facilitam a prática de crimes.



Dicas para manter-se seguro

- Evite expor dados pessoais, como nome completo, telefone, endereço, local de trabalho ou lugares onde frequenta;
- Tenha muito cuidado ao se encontrar com amigos virtuais, pois podem ser pessoas mal intencionadas;
- Mesmo que você conheça algum amigo virtual há bastante tempo, isso não garante que seja uma pessoa confiável ou que as informações dadas por ele sejam verdadeiras;
- Caso receba mensagens ou imagens agressivas que tentem forçar uma conversa, bloqueie o usuário, denuncie e peça ajuda;
- Confira se suas conversas estão sendo gravadas no histórico do serviço. Saiba que é possível apagar e não gravar se preferir;
- Caso queira esclarecer dúvidas, acesse: www.canaldeaajuda.org.br



Webcam

A *webcam* é um dispositivo que pode ser acoplado ao computador e permite que o usuário possa ver quem está do outro lado da tela e/ou ser visto. Permite que pessoas de diferentes lugares do planeta sintam-se mais próximas. Também estão presentes em celulares, *tablets*, videogames e até em relógios.



Aproveite!

- Permitem a comunicação com imagens em tempo real, independentemente das distâncias;
- Você pode escolher com quem conversar e pode bloquear contatos indesejados;
- Pode ver ao vivo amigos, parentes distantes de forma bem econômica.



Cuidado!

- Pessoas mal intencionadas podem se utilizar deste recurso para capturar imagens íntimas de alguém;
- Nunca podemos confiar totalmente em quem está do outro lado da tela. Pessoas podem cometer crimes utilizando imagens de outros usuários para enganar a vítima.
- A pessoa para quem você se mostra intimamente pode publicar suas imagens ou te chantagear.
- Você deixaria uma pessoa estranha entrar na sua casa? E por que permitir que ela entre através do uso da *webcam*?



Dicas para manter-se seguro

- Utilize a *webcam* preferencialmente com pessoas que conhece presencialmente;
- Ainda que use *webcam* apenas com amigos e familiares, tenha muito cuidado com a forma como você se expõe;
- Pense muito bem antes de ligar a *webcam*. Namorar pela Internet pode ser divertido, mas também muito arriscado;
- Converse com seus filhos ou alunos sobre o uso consciente da *webcam*;
- Para mais informações, envie uma mensagem através do endereço www.canaldeajuda.org.br



Sites de Redes Sociais

São *sites* que permitem criar uma página pessoal na Internet, encontrar amigos, participar e criar comunidades para compartilhar gostos e ideias. Possibilitam atualizar e divulgar um espaço pessoal na Internet com textos, fotos e vídeos. Atualmente, é um dos espaços preferidos pelos Internautas brasileiros de todas as idades para se encontrarem e se relacionarem pela Internet. Exemplos: Orkut, Twitter, MySpace, Hi5, Facebook...



Aproveite!

- Facilitam a interação entre pessoas de qualquer lugar do mundo;
- Permitem o compartilhamento de ideias e interesses em comum;
- Permitem discussões e debates com liberdade de expressão sobre temas variados;
- Fornecem muitos recursos para divulgar e trocar imagens, vídeos, *sites* e recados.



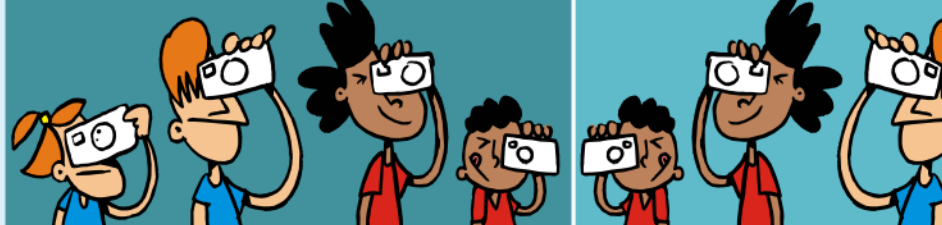
Cuidado!

- Quando divulgamos informações pessoais na Internet, elas se tornam públicas;
- Após publicar algo na Internet, é impossível voltar a escondê-lo;
- Não exponha detalhes de sua vida. Sua intimidade é preciosa e não deve ser aberta para qualquer um;
- Os “cadeados” e bloqueios de acesso não são 100% seguros. Fique atento ao que você publica e com quem compartilha!
- Infelizmente as redes sociais podem ser utilizadas por pessoas mal intencionadas para a prática de crimes;
- Seus dados ficam gravados, podendo ser roubados e manipulados para o ofender ou chantagear. Muito cuidado com suas senhas!



Dicas para manter-se seguro

- Ajuste as configurações de privacidade do seu perfil. Isso aumenta o seu controle sobre o uso das informações;
- Você distribui seu endereço, suas fotos ou número de telefone para qualquer um na praia, na praça, no ônibus ou no mural da escola? E por que faria isso na Internet?
- Evite comentar sobre detalhes de horários e lugares onde estará. Faça isso por telefone ou por *e-mail* apenas com quem conhece pessoalmente;
- Valorize também a qualidade de amigos e não apenas a quantidade;
- Evite aceitar encontro presencial com quem não conhece;
- Troque sua senha periodicamente;
- Caso seja agredido por estranhos, configure sua conta para bloquear os contatos indesejados;
- Se visualizar conteúdos acessíveis publicamente na Internet que sejam suspeitos de serem racistas ou com cenas de violência contra crianças, denuncie em www.denunciar.org.br



Blogs, Fotologs e Microblogs

São espaços na Internet que podem ser criados por qualquer internauta para publicar suas ideias, fotos, preferências, desejos e expectativas. Nos *blogs* e *fotologs*, é possível debater diversos temas, fazer comentários, participar de enquetes, compartilhar *links* e todas as informações que considerarmos interessantes. Podem ser individuais ou coletivos, e geralmente são gratuitos. Os *fotologs* são utilizados para publicação de fotos, inclusive através do celular.



Aproveite!

- Permitem que qualquer pessoa tenha um espaço na Internet;
- Ampliam a liberdade de expressão e facilitam a troca de informações entre as pessoas de todo o mundo;
- Estimulam a leitura, a escrita e a criatividade;
- O uso é simples e podem ser atualizados a qualquer momento com muita rapidez;
- As pessoas podem interagir comentando ideias e publicações.



Cuidado!

- Quando publicamos algo, é muito difícil remover completamente da rede. Qualquer um pode ver, gravar e usar sem nosso controle. Pense muito bem antes de publicar!
- Muito cuidado com o que você fala! Não confunda liberdade de expressão com ofensas!
- Lembre-se de que você é responsável legalmente por tudo o que publica.



Dicas para manter-se seguro

- Seja educado e cordial ao publicar conteúdos ou comentários na Internet;
- Evite expor dados pessoais como endereço, telefone, nome completo, local de trabalho e etc;
- Você publica fotos e imagens íntimas em qualquer espaço público? Pense muito bem antes de postar algo na Internet;
- Cuidado com as fotos que posta, elas podem ser modificadas e usadas contra você;
- Você pode usar a moderação dos comentários para evitar mensagens desrespeitosas em seu *blog*;
- Uma vez publicadas, todas as informações podem ser gravadas e postadas novamente por outras pessoas, mesmo que você venha a apagar seu *blog* ou *fotolog* da rede.



Redes P2P

Conhecida como P2P (do inglês, *peer-to-peer* = ponto a ponto), é uma rede descentralizada de computadores que podem trocar entre si informações como músicas, vídeos, textos e programas. Os usuários das redes P2P fornecem e recebem dados ao mesmo tempo, ou seja, são servidores e clientes simultaneamente. Exemplo: Emule, rede *Torrent*. Além das redes P2P, há os *sites* de compartilhamento de arquivos.



Aproveite!

- Agilidade incrível para trocar arquivos com outros internautas;
- Não dependem de um servidor que controle os dados;
- Permitem compartilhar seus conteúdos preferidos e adquirir outros.



Cuidado!

- Você pode receber arquivos impróprios e agressivos sem desejar;
- Os arquivos podem ter nomes falsos para disfarçar conteúdos ilegais;
- Podem facilitar a invasão do seu computador para roubo de dados.



Dicas para manter-se seguro

- Faça buscas com cuidado e confira o nome e a origem dos arquivos;
- Leia com atenção o contrato de uso dos programas e não permita a divulgação de seus dados pessoais;
- Muito cuidado ao baixar arquivos que sejam executáveis (.exe) ou compactados;
- Busque informações sobre a permissão para gravar e divulgar os arquivos disponíveis na rede;
- Caso receba por engano conteúdos agressivos e que contenham agressões contra crianças, adolescentes, racismo ou intolerância religiosa, denuncie no www.denunciar.org.br



Jogos On-Line

São jogos que permitem a interação de vários participantes ao mesmo tempo, conectados pela Internet. Podem ser jogos de diferentes tipos com ação em equipe e conversas entre os jogadores por meio de mensagens e *chat*. Alguns jogos podem durar meses e, cada vez que se conecta, o usuário pode continuar de onde parou.



Aproveite!

- Ajudam a desenvolver habilidades de coordenação motora, estimulam a criatividade e incentivam a leitura;
- Permitem interação com jogadores em diferentes lugares do mundo;
- Podem ser divertidos e educativos.



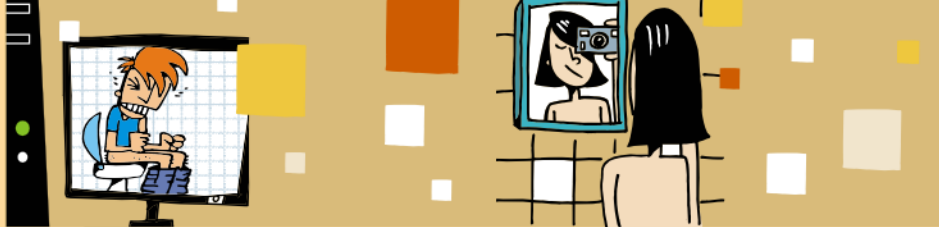
Cuidado!

- Jogar em excesso prejudica a saúde e os estudos, podendo até causar dependência;
- Há criminosos que fingem ser jogadores para prejudicar pessoas e roubar dados;
- Alguns estimulam a violência e práticas criminosas;
- Existem jogos com forte apelo ao consumo para a compra de seus produtos e você pode acabar perdendo o controle sobre seus gastos.



Dicas para manter-se seguro

- Não aceite provocações e disputas que possam trazer problemas na "vida real";
- Verifique sempre a idade mínima indicada para cada jogo;
- Ao terminar de jogar, lembre-se sempre de clicar em "sair" para evitar que roubem seus dados;
- Caso receba mensagens agressivas e com conteúdos impróprios, denuncie à central de suporte do jogo em questão;
- A imersão digital das crianças é importante, mas também estimule seu filho a praticar outras atividades, como esportes, passeios, brincadeiras e leituras fora do computador.
- Estabeleça regras e horários de uso juntamente com a criança ou o adolescente.



Privacidade

Atualmente, o número de serviços e ferramentas de interação social na Internet vem aumentando. Com isso, cresce também o nível de exposição das pessoas na rede. É fundamental que os usuários fiquem atentos para os dados que disponibilizam na Internet e aos termos de uso de cada serviço que utiliza.

Cuidado

- Empresas que gerenciam contas de *e-mail*, redes sociais e outros serviços podem armazenar e comercializar seus dados e informações pessoais. Fique atento aos termos de uso e de privacidade de tudo o que utiliza na Internet;
- O que você publica em seu perfil pode ser visto por pessoas de várias partes do mundo, inclusive por usuários mal intencionados. Configure suas contas para garantir mais privacidade das suas informações;
- O uso da webcam pode ser um ótimo meio de se sentir mais próximo de pessoas que estão distantes. Porém, usá-la de forma equivocada facilita que alguém grave suas imagens para tirar proveito disso.



Dicas para manter-se seguro

- Orientar crianças e adolescentes a não expor informações como endereço, telefone e nome da escola. Quanto menos informações pessoais se coloca na rede, mais seguro o usuário está;
- Não registrar ou publicar fotos íntimas que possam causar algum tipo de constrangimento. Uma vez na Internet, é muito difícil remover completamente da rede;
- Não adicionar pessoas desconhecidas;
- Não compartilhar senhas pessoais, mesmo que seja com pessoas de confiança, pois é somente a partir dela que é possível acessar as contas e páginas pessoais de forma segura;
- Não abrir *e-mails* que não considerem seguros. Mesmo não sendo intencional, vírus também podem ser enviados por amigos;
- Manter o antivírus sempre atualizado;
- Leia os termos de uso e termos de privacidade dos serviços que usa na rede.



Uso excessivo

Cada vez mais, boa parte das nossas atividades acontecem *on-line*. As pessoas estudam, ouvem música, assistem a filmes, jogam, namoram, se divertem e se comunicam através da Internet, seja pelo computador, celular, videogame ou *tablet*. Para usufruir das tecnologias sem prejuízos nem danos, é preciso saber usar com responsabilidade e limites, para que o uso em excesso não venha a prejudicar a saúde, os estudos, o trabalho e os relacionamentos.

Cuidado

- Usar a Internet durante todo o tempo livre, deixando até de dormir para ficar conectado, pode atrapalhar suas atividades diárias;
- Ficar sempre ansioso para conectar e/ou jogar pode ser um sinal de que você está perdendo o controle do seu uso;
- Ficar horas e horas, por exemplo, num mesmo jogo, dias seguidos fazendo a mesma coisa pode estar fazendo do seu uso pouco criativo;
- Se você deixa tudo de lado para estar conectado ou jogando, deixando amigos e outras atividades sempre para depois, você pode perder bons momentos da vida.



Dicas para manter-se seguro

- Em alguns momentos, prefira fazer coisas divertidas e prazerosas desconectado, como passear, conhecer lugares novos, praticar um esporte, ir ao cinema, encontrar amigos em uma festa, *shopping*, clube, praia e etc.
- Passar muitas horas jogando *on-line* ou na frente do computador, *tablet*, *notebook* ou *smartphone* pode ser um refúgio para tentar esquecer problemas e evitar contatos diretos com outras pessoas. Se este for o seu caso, vale a pena procurar alguém em quem confie para desabafar ou mesmo buscar suporte de um psicólogo;
- Organize seu tempo para se dedicar às suas atividades, inclusive as que realizará durante o tempo livre;
- Se você é responsável por crianças ou adolescentes, negocie e crie com eles as regras e horários saudáveis para o uso da Internet;
- Já parou para pensar na quantidade de horas que ficamos ligados a alguma tela? Em casa, na rua, na escola... Em todo lugar há uma tela! Fique atento para escolher com autonomia e cuidado o que ver nas telas e por quanto tempo.

PERIGOS NA REDE



Cibercrime - Crime Digital

Uso das novas tecnologias para ações ilícitas como roubo, chantagem, calúnia, difamação e violação aos Direitos Humanos fundamentais. O ciberespaço é um ambiente público que reflete a diversidade e complexidade da sociedade, tanto nas qualidades como nas práticas ilegais.

Cuidado

- Como todo crime, prejudica as pessoas moralmente ou financeiramente;
- Quem pratica crimes pela Internet se aproveita da falsa sensação de anonimato e impunidade;
- É preciso respeitar as leis *on-line* para manter a Internet como um espaço público livre e seguro. Lembre-se de que a Internet não é uma “terra sem lei”.



Dicas para manter-se seguro

- Divulgue o mínimo de informações pessoais na Internet, seja discreto;
- Troque senhas com frequência e evite utilizar informações óbvias ao criá-las, como datas de aniversário ou números de telefone. Além disso, não compartilhe suas senhas, nem mesmo com pessoas que você confia. Isso pode evitar problemas!
- Não deixe sua conta de *e-mail* ou da rede social conectada quando não estiver usando o computador. Sempre utilize a opção “sair” após utilizar qualquer serviço *on-line*!
- Não grave arquivos confidenciais ou dados pessoais em LAN houses. Use *pen drive* ou CD e apague da área de trabalho os arquivos que abriu;
- Caso perceba alguma irregularidade em seu extrato bancário ou cartão de crédito, comunique imediatamente ao seu banco ou operadora o que aconteceu;
- Nas compras pela Internet, dê preferência para pagamentos com cartão de crédito ou boleto bancário e sempre procure empresas conhecidas e respeitadas;
- Desconfie de ofertas mirabolantes. O “conto do bilhete premiado” já chegou à Internet;
- Veja mais dicas em www.safernet.org.br

PERIGOS NA REDE



Ciberbullying/Ofensas

São repetidas ofensas, ameaças e ridicularizações que ocorrem entre crianças e adolescentes através de telefone celular, *e-mail*, *blog* e redes sociais. Com adultos, este tipo de violação não é caracterizado como *ciberbullying*, e sim como crimes de Ameaça (Art. 147 do Código Penal), Calúnia (Art. 138 do Código Penal), Difamação (Art. 139 do Código Penal) e Injúria (Art. 140 do Código Penal). *Ciberbullying* não é brincadeira, pois, ao brincar, é preciso que todas as partes se divirtam e se respeitem.

Cuidado

- Algumas vezes a agressão pode ser anônima, sendo mais difícil identificar o autor;
- Essa violência pode se prolongar por anos;
- Curtir e compartilhar mensagens, fotos ou vídeos que agridem outras pessoas são formas de compactuar com o *ciberbullying*;
- Violências como essa podem deixar marcas para sempre!
- A violência através da Internet ou do celular também machuca muito;
- Ao praticar *ciberbullying*, você pode ser responsabilizado por esta atitude e até mesmo sofrer punições.



Dicas para manter-se seguro

- Se seu filho ou aluno está passando por este tipo de situação, ofereça apoio e mostre que ele não está sozinho;
- Provocações e ofensas na Internet não devem ser respondidas. Ao passar por isso, grave todas as mensagens ou imagens;
- Imagens ou comentários ofensivos podem ser denunciados ao próprio *site*, sendo possível bloquear o contato no celular, *chat*, *e-mail* e redes sociais.
- Cuidado com o que escreve e com as imagens que divulga na rede. Conecte-se com respeito!
- Se perceber que algum colega de seu filho está sofrendo agressões pela Internet, encoraje-o a denunciar e ajude-o;
- Os pais podem ser responsabilizados judicialmente pelas agressões que os filhos cometem, porém o mais adequado é tentar resolver essa situação com diálogo e orientação, já que crianças precisam do cuidado dos adultos;
- Em casos de *ciberbullying*, é importante buscar diálogo com todas as partes envolvidas (autores, vítimas, pais/responsáveis e a escola, quando for o caso);
- O futuro da Internet depende do que se faz com ela hoje. Ao usar a Internet para agredir e humilhar alguém, estimulam-se novas leis de controle e proibição. Utilize-a com responsabilidade e respeito!
- Mais dicas e orientações em www.canaldejuda.org.br

PERIGOS NA REDE



Sexting

Sexting é um termo originado da união de duas palavras em inglês: *sex* (sexo) + *texting* (envio de mensagens). É um fenômeno recente no qual adolescentes e jovens usam celulares, câmeras fotográficas, redes sociais e demais recursos digitais para produzir e enviar fotos sensuais de seu corpo (nu ou seminú). Envolve também mensagens de texto eróticas *on-line*, com convites e insinuações sexuais.

Cuidado

- Infelizmente não são apenas os amigos que podem ter acesso ao que é divulgado na Internet e sim pessoas de diferentes locais do mundo;
- Atuais e futuros colegas de escola e de trabalho, parentes, inimigos, estranhos e até criminosos podem ver, copiar e manipular o que você divulga na Internet para, no futuro, usar isso contra você;
- Uma vez *on-line*, perde-se completamente o controle da foto ou texto que se publica;
- Pode parecer uma brincadeira, porém este tipo de mensagem sensual coloca sua privacidade em risco;
- Essas fotos podem expor sua vida para pessoas que você nem gostaria de conhecer.



Dicas para manter-se seguro

- Jamais se deixe levar por pressões para produzir ou publicar imagens sensuais;
- Tudo o que fazemos *on-line* tem consequências também fora da Internet. Pense muito bem antes de publicar;
- Converse com seus filhos sobre sexualidade e privacidade. Esclareça as dúvidas e mostre que você pode escutá-lo!
- Não há nada de errado em falar e discutir sobre sexualidade. O erro é não se proteger e não se informar sobre como manter relações saudáveis dentro e fora do ciberespaço;
- Proteja seus direitos sexuais e não facilite agressões;
- Pais: orientem e dialoguem com seus filhos para conhecer o que fazem *on-line*. Os valores e limites de sua família precisam ser discutidos também em relação aos comportamentos *on-line*. Converse com seus filhos sobre as noções de privacidade e de comportamento de risco para construir limites como proteção e não como proibição;
- Pais e educadores: saibam que vocês não precisam ser experientes em tecnologia, basta transpor a cidadania também para este novo ciber-espaço público.
- Se quiser mais orientações sobre o assunto, acesse: www.canaldeaajuda.org.br

PERIGOS NA REDE



Aliciamento sexual infantil on-line

O aliciamento sexual infantil consiste em conversas e atitudes sexualizadas por parte de um adulto com uma criança ou adolescente. Isso pode vir a acontecer também em ambientes *on-line*, através do envio de imagens de conotação sexual e conteúdos impróprios para o público infanto-juvenil através de aparelho celular, *e-mail*, redes sociais, *blog*, salas de bate-papo e comunicadores instantâneos.

Cuidado

- Os aliciadores fingem ser amigos virtuais, são "amáveis" nas primeiras conversas de *chat* e Comunicador Instantâneo (MSN...);
- Se passam por crianças nas Redes Sociais e conhecem o mundo infantil;
- Alguns se apresentam como adultos e enviam cenas de sexo com desenhos para estimular fantasias impróprias;
- Elogiam demais para ganhar confiança e pedir informações como nome de escola, endereço, celular e fotos;
- Pedem cada vez mais fotos até solicitarem conversas com *webcam*;
- Manipulam fotos e colocam o rosto da vítima em cenas de sexo;
- Ameaçam divulgar na Internet as fotos manipuladas para humilhar diante de amigos e familiares em *sites*;
- Ameaçam saber o endereço para agredir presencialmente em casa ou na escola;
- Nos piores casos, pode terminar em sequestro e abuso sexual.



Dicas para manter-se seguro

- Cuidado, nunca teremos certeza de quem está por trás de um perfil, de um *e-mail* ou apelido;
- Não responda as mensagens de desconhecidos e grave quando houver ameaça ou imagens violentas;
- Jamais aceite convite para encontrar presencialmente um amigo virtual sem autorização. Mesmo com os responsáveis, vá a local público e movimentado;
- Bloqueie o contato dos agressores no celular, *chat*, *e-mail* e redes de relacionamento;
- Se algum conhecido está sendo vítima, encoraje-o a denunciar e ajude-o a buscar apoio;
- Quando o conteúdo envolve crianças e adolescentes na Internet, você deve denunciar em www.denunciar.org.br, ligar para o Disque 100, ir a uma Delegacia Especializada, Ministério Público ou se dirigir ao Conselho Tutelar mais próximo;
- Lembre-se de que somente denunciando às autoridades é que os criminosos poderão ser punidos. Jamais tente fazer justiça com as próprias mãos.

PERIGOS NA REDE



Conteúdos Impróprios

São conteúdos considerados impróprios para a fase em que uma criança ou um adolescente se encontra. Um dos motivos de maior preocupação dos pais e educadores em relação à Internet é o tipo de conteúdo e o tempo que os filhos/alunos permanecem na rede.

Cuidado

- É importante compreender que alguns conteúdos que uma criança ou adolescente encontra na rede podem ser prejudiciais para o seu desenvolvimento psicológico e sexual;
- A exposição a determinados conteúdos pode facilitar o contato com pessoas mal intencionadas;
- Programas de bloqueio de conteúdos não são 100% eficazes. É importante orientar crianças e adolescentes a respeito de suas dúvidas e de como se prevenir dos riscos;
- Evite abrir arquivos de desconhecidos, seja no *e-mail*, *chat*, comunicador instantâneo ou redes de compartilhamento;
- Confira a idade permitida para cada jogo, *site* de rede social ou qualquer outro serviço *on-line* antes de autorizar o uso;



Dicas para manter-se seguro

- A melhor estratégia de proteção é a orientação de crianças e adolescentes, criando regras de uso em casa, na escola e na LAN house;
- Crianças e adolescentes podem utilizar a Internet sim, mas com orientação dos pais e educadores, com limites de tempo para navegar e de conteúdo;
- Participar ativamente de todas as atividades realizadas pelos filhos, inclusive sobre os serviços que eles utilizam no ciberespaço, é uma estratégia para orientá-los;
- Orientar crianças e adolescentes a não abrir arquivos desconhecidos, seja por *e-mail*, *chat*, comunicador instantâneo e redes de compartilhamento;
- Caso visualize algum conteúdo que viole os Direitos Humanos, denuncie em www.denunciar.org.br
- Para esclarecer dúvidas sobre situações de risco e perigos, acesse: www.canaldeajuda.org.br

PERIGOS NA REDE



Roubo de Dados/Invasão

Utilizar de dados pessoais como senha, perfil, comunidade, avatar, personagem ou *e-mail* de um usuário sem a autorização ou consentimento para qualquer fim pode ser considerado crime.

Cuidado

- Atente-se periodicamente para os termos de uso e privacidade dos *sites* que você utiliza;
- Invadir sites, contas de *e-mail* e demais serviços *on-line* vai de encontro às leis vigentes no país e pode ser considerado crime;
- Gera insegurança e constrangimento para os internautas;
- Se passar por outra pessoa na Internet para ofender e humilhar também é crime;
- Ao fazer compras *on-line*, busque referências para verificar se o *site* é seguro para colocar suas informações.



Dicas para manter-se seguro

- Nunca abra arquivos anexos de remetentes desconhecidos;
- Não instale programas que sejam enviados por pessoas que você não conhece;
- Mantenha o antivírus e o *firewall* sempre atualizados;
- Os navegadores de Internet livres como o Mozilla Firefox podem ser mais seguros;
- Não acredite em todas as informações que receber;
- Esteja sempre em alerta, não adicione pessoas que você não conheça e suspeite de *e-mails* desconhecidos;
- Informação é a base de tudo, portanto, esteja sempre atualizado sobre os cuidados quanto à utilização segura da Internet;
- Desconfie de anexos sem comentários no corpo do *e-mail*;
- Troque periodicamente suas senhas;
- Denuncie ao próprio *site* quando houver perfis falsos e páginas que agridam outros usuários;
- Caso queira esclarecer dúvidas, acesse: www.canaldeajuda.org.br

PERIGOS NA REDE



Justiceiros Virtuais

Algumas pessoas tentam "fazer justiça" com as próprias mãos, invadindo *sites* para tirar alguns conteúdos da Internet. Em vez de buscar os meios legais para resolver o problema, tentam solucioná-lo por conta própria e quase sempre dificultam os trabalhos de investigação das autoridades. Além disso, colocam-se em risco ao desafiar criminosos perigosos.

Cuidado

- Iludem e seduzem jovens internautas para serem "heróis na Internet";
- Muitas vezes cometem crimes para combater outros crimes;
- Podem colocar pessoas em risco sem que elas se deem conta da gravidade do problema;
- Entram em disputa direta com redes de pessoas perigosas;
- Alguns usam ameaças e chantagem para manter pessoas "presas" aos grupos de justiceiros.



Dicas para manter-se seguro

- Cuidado com as comunidades ou usuários que se consideram heróis da Internet, detetives digitais ou ciberpoliciais;
- Não faça justiça com o seu próprio *mouse*;
- Lembre-se de que todos têm direito de se expressar livremente, respeitando as leis e os Direitos Humanos;
- Se for ameaçado, comunique imediatamente aos seus familiares, à polícia e denuncie;
- Se algum conhecido está envolvido com justiceiros virtuais, esclareça-o sobre os riscos e oriente-o a comunicar às autoridades em caso de ameaças ou intimidações;
- Para transformar a Internet em um espaço mais seguro e legal, seja educado e denuncie quando presenciar algo suspeito;
- Em caso de roubo, difamação e fraude, procure uma delegacia especializada em crimes eletrônicos;
- Em caso de visualizar conteúdos com cenas de violência contra crianças, racismo, intolerância de gênero ou religiosa, denuncie em www.denunciar.org.br;
- Saiba mais sobre o trabalho das autoridades brasileiras através do *site* da Polícia Federal (www.dpf.gov.br), do Ministério Público Federal (www.mpf.gov.br) e dos Ministérios Públicos e Polícias de seu estado.
- Mais dicas em netica.org.br



Canal de ajuda / Helpline

O Helpline BR é um serviço de utilidade pública oferecido pela SaferNet Brasil em parceria com a Secretaria de Direitos Humanos da Presidência da República. Nosso objetivo é usar a tecnologia em favor da proteção dos direitos de crianças e adolescentes que estejam preocupadas ou vivenciando situações de perigo *on-line*. Acesse www.canaldeajuda.org.br e converse com nossa equipe!



Agora vamos ver se você já sabe se proteger na Internet?

1. O que você acha de fazer amizades com pessoas desconhecidas (amigos virtuais)?

- a) Acho ótimo, adoro fazer amizades!
- b) Acho ruim, as pessoas podem fingir ser quem não são e podem me prejudicar.
- c) Acho legal fazer amizades virtuais, porém é importante ter muito cuidado com minha imagem, meus dados pessoais e meus segredos.

2. Uma pessoa de sua turma postou comentários maldosos sobre você. Isso o deixou muito triste e com vergonha. O que você faz?

- a) Respondo aos comentários da mesma forma, afinal, tenho que revidar.
- b) Conto aos meus pais e procuro a escola para que eles possam me ajudar.
- c) Não faço nada e tento faltar às aulas até que meus colegas esqueçam.

3. Você acha que se expor na *webcam* para alguém que conhece é algo perigoso?

- a) Acho importante sempre refletir se de fato eu posso confiar na pessoa que está do outro lado do computador e se não vou me comprometer me expondo na *web*, mesmo com pessoas aparentemente confiáveis.
- b) Talvez... É só não se expor para desconhecidos.
- c) Não. Se eu confio na pessoa, posso me expor do jeito que quiser.

4. A Internet ocupa quanto tempo do seu dia?

- a) O dia todo, não consigo me desconectar! E quando estou longe, não paro de pensar na Internet.
- b) Costumo navegar na Internet durante todo o tempo livre até a hora de dormir.
- c) Apenas parte do meu tempo livre. Não costumo desmarcar nada para ficar na Internet!

No Helpline, você pode conversar com uma equipe de psicólogos especializada para orientar e esclarecer dúvidas ou situações como as que você aprendeu no **QUIZ!** A orientação pode ser feita por e-mail ou chat. Acesse www.canaldeajuda.org.br
É gratuito e seguro!

Denuncie

Assim como na rua, nas praças e nos espaços “off-line”, é muito importante que os usuários estejam cientes a respeito de como proceder em situações de risco nos ambientes digitais. A Internet não é uma terra sem lei. As pessoas mal intencionadas que cometem crimes *on-line* podem e devem ser responsabilizadas legalmente pelos seus atos. As leis e regras de convivência devem valer sempre para as relações entre as pessoas, seja na Internet, na escola, no trabalho, na rua ou em qualquer outro espaço. Ao presenciar algum crime na Internet, temos o dever cívico de denunciar.



Como denunciar

Para denúncias de crimes contra os Direitos Humanos na Internet, acesse:

www.denunciar.org.br



Copie o link que está na barra de endereços

- Não precisa se identificar, a denúncia é anônima;
- O código fornecido no ato da denúncia deve ser guardado com você cuidado;
- Para outras violações, você pode buscar orientações sobre como proceder através deste link: www.netica.org.br

Crimes Contra os Direitos Humanos na Internet?

Denuncie!

“Você está em: Tipo de conteúdo”

Tipo de conteúdo

- Pornografia Infantil
- Racismo
- Apologia e Incitação a crimes contra a Vida
- Xenofobia
- Neo Nazismo
- Maus Tratos Contra Animais
- Intolerância Religiosa
- Homofobia
- Tráfico de Pessoas

Apologia e Incitação a crimes contra a Vida
Qualquer tipo de conteúdo publicado na Internet que promova, incite ou faça apologia a violência contra seres humanos.

Página da Internet
<http://www.endereconaweb.com.br>

Código único

Denunciar

SaferNet Brasil

- Onde mais é possível denunciar violações contra os Direitos Humanos e contra os direitos das crianças e adolescentes?

DISQUE 100

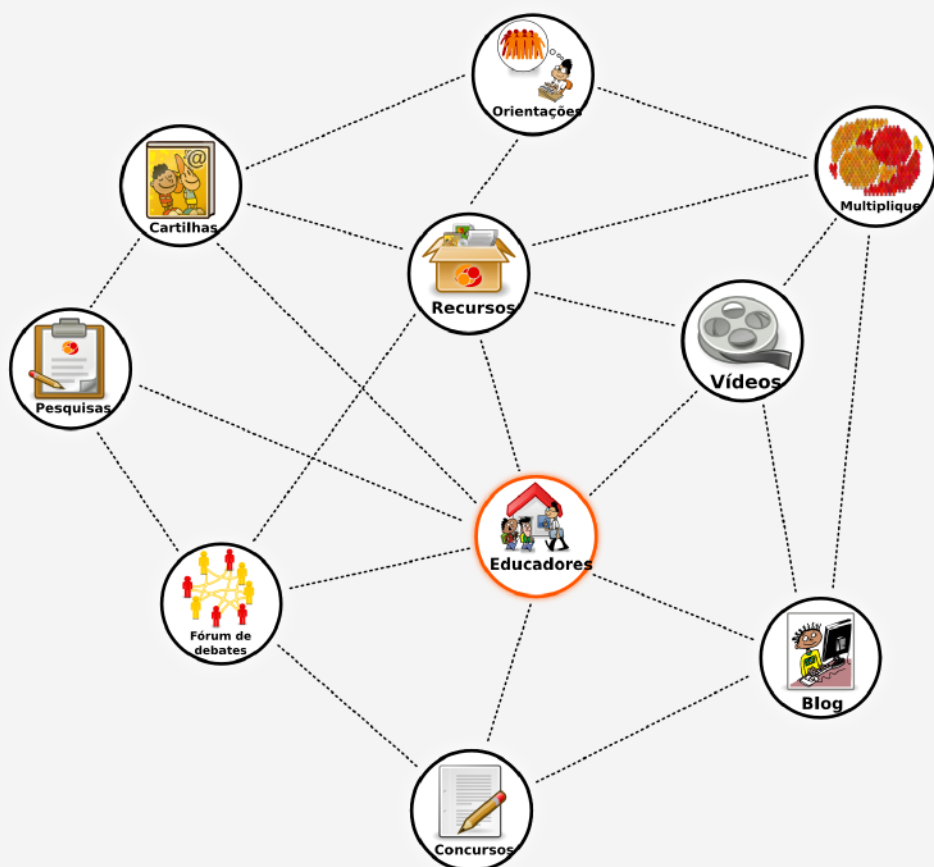
CONSELHO TUTELAR

MINISTÉRIO PÚBLICO

DELEGACIA DE POLÍCIA

Conheça Também...

Os demais recursos pedagógicos que a SaferNet disponibiliza gratuitamente para pais e educadores, com dicas para educação em Direitos Humanos, cidadania digital e segurança na Internet.



Acesse: netica.org.br/educadores

A SaferNet Brasil é uma associação civil sem fins lucrativos e econômicos, sem vinculação político-partidária, religiosa ou racial, fundada em 20 de dezembro de 2005, por um grupo formado por cientistas da computação, professores universitários, pesquisadores e bacharéis em Direito.

A SaferNet Brasil criou e mantém a Central Nacional de Denúncias de Crimes Cibernéticos (www.denunciar.org.br) que, desde 29/03/2006, é operada em parceria com o Ministério Público Federal e atualmente em cooperação também com a Polícia Federal, Secretaria de Direitos Humanos da Presidência da República, Conselho Nacional dos Procuradores Gerais de Justiça e com o Comitê Gestor da Internet no Brasil. A Central oferece o serviço gratuito de recebimento, processamento, encaminhamento e acompanhamento *on-line* de denúncias anônimas sobre crime ou violação aos Direitos Humanos praticado por meio da Internet.

A Central Nacional de Denúncias de Crimes Cibernéticos recebe uma média de 2.500 denúncias (totais) por dia envolvendo páginas suspeitas de conter evidências de crimes de pornografia infantil, racismo, neonazismo, intolerância religiosa, apologia e/ou incitação a crimes contra a vida e homofobia.

A SaferNet Brasil também desenvolve um conjunto de ações focadas na área de prevenção e educação para promover o uso ético e responsável da Internet no Brasil. A SaferNet entende que atuar na prevenção é uma forma eficaz para reduzir a incidência de violações de direitos neste novo espaço público chamado ciberespaço. Promover o uso ético e responsável permite gerar uma navegação mais segura e ao mesmo tempo faz com que possamos aproveitar mais e melhor das infinitas qualidades que a Internet oferece a todas as idades, seja para estudar, trabalhar, brincar, comunicar-se ou simplesmente passar o tempo. Medidas educativas e campanhas de prevenção precisam ser constantes e, se possível, desde o primeiro clique.

Sabemos que a Internet é uma ferramenta fantástica, que pode contribuir muito para o desenvolvimento cognitivo, social e emocional de nossas crianças. Porém, como toda tecnologia que se propõe a aproximar pessoas, também pode colocar em risco a segurança e a saúde de crianças, jovens e adultos, quando não orientados sobre o uso ético e responsável da rede. Por essa razão, o uso da Internet pelas crianças e adolescentes precisa ser estimulado conjuntamente com ações efetivas de orientação e acompanhamento dos pais e educadores.

Conheça mais sobre as nossas ações: www.safernet.org.br

Testemunhou algum crime na Internet, denuncie: www.denunciar.org.br

Software Livre

A Central Nacional de Denúncias de Crimes Cibernéticos, um dos principais projetos da SaferNet Brasil, possui um sistema automatizado de gestão de denúncias, que permite ao internauta acompanhar, em tempo real, cada passo do andamento do seu registro. O sistema, único na América Latina e Caribe, foi desenvolvido pela equipe de TI (Tecnologia da Informação), baseado em *Software Livre*.

Por que *Software Livre*?

A SaferNet Brasil compartilha da ideologia da rede de *Software Livre*, que defende a liberdade do usuário para executar, distribuir, modificar e repassar as alterações, sem depender de permissão do autor do programa. Para nós é fundamental ter o direito de conhecer plenamente o funcionamento de cada programa utilizado.

Para entender este conceito, você deve pensar em liberdade, ou melhor, em pelo menos quatro liberdades que são asseguradas aos usuários. Elas foram estabelecidas pela Free Software Foundation (www.fsf.org) como os requisitos mínimos para que um *software* seja considerado livre. São elas:

- A liberdade de executar o programa, para qualquer propósito;
- A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades;
- A liberdade de redistribuir cópias de modo que você possa beneficiar o próximo;
- A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie.

Para que o usuário possa usufruir de algumas dessas liberdades (como a liberdade de estudar o programa e a liberdade de modificá-lo), é necessário acesso ao código-fonte.

Código-fonte é uma das etapas da criação de um programa de computador. É nele onde o programador escreve, passo a passo, as instruções que o *software* deverá executar. O importante é que, no código-fonte, essas instruções estão escritas de forma que os seres humanos possam compreender, enquanto que o arquivo executável (o programa em si) não pode ser compreendido pelas pessoas, por estar em linguagem binária. Os distribuidores de *software* não livre entregam ao usuário apenas o executável, impedindo o usuário de estudar como o programa funciona e modificá-lo.

Note que em nenhum dos itens se fala de preços ou custos. É um erro comum achar que *Software Livre* é *software* gratuito. É verdade, sim, que a maioria dos Softwares Livres é distribuída gratuitamente, mas essa é uma consequência esperada da terceira e da quarta liberdades, que permitem distribuir o programa com ou sem modificações, sem restrições.

O *Software Livre* pode ser usado em qualquer tipo de sistema computacional, para qualquer tipo de trabalho ou atividade, sem que seja necessário comunicar ao desenvolvedor ou a qualquer outra entidade em especial. O sistema operacional GNU/Linux e o navegador Firefox são os exemplos mais conhecidos de *Softwares Livres*.

Benefícios para os usuários:

- Poder utilizar o *software* para qualquer finalidade;
- Ter acesso ao código fonte e poder modificá-lo, sem restrições;
- Poder copiá-lo e executá-lo em quantas máquinas desejar (o *software* não livre, em geral, impõe restrições quanto a isso);
- Poder distribuí-lo;
- Contar com estabilidade, segurança, e correções de falhas de forma ágil;
- Ter o computador equipado com *software* de qualidade a um custo baixo ou nulo;
- Não depender das restrições impostas pelas licenças de *softwares* proprietários e de preços abusivos das novas versões;
- Não depender de apenas um fornecedor;
- Ficar livre da pirataria e ter todo o seu *software* legalizado;
- Incentivar o desenvolvimento de tecnologia local;
- Interagir e compartilhar soluções com comunidades, sejam físicas ou virtuais;
- Lutar contra o monopólio de grandes corporações que tentam se apropriar do conhecimento intelectual coletivo para benefício privado.

Para a SaferNet Brasil, utilizar *Software Livre* é a única maneira de assegurar a continuidade dos programas utilizados, garantir que os programas poderão ser adaptados às necessidades particulares da organização, e ter certeza que o programa faz aquilo que esperamos que ele faça, sem rotinas desconhecidas ou comportamentos inesperados.

Fontes: www.softwarelivre.org e www.psl-ba.softwarelivre.org

Copyright © 2013 SaferNet Brasil

Esta obra é licenciada pela Creative Commons By-NC-SA
<http://creativecommons.org/licenses/by-nc-sa/3.0/br>



www.SaferNet.org.br/cartilha

Patrocínio:

PROGRAMA
PETROBRAS
DESENVOLVIMENTO
& CIDADANIA



GOVERNO FEDERAL
BRASIL
PAÍS RICO E PAÍS SEM POBREZA

Cooperação:

MPF
Ministério Público Federal



Realização:

