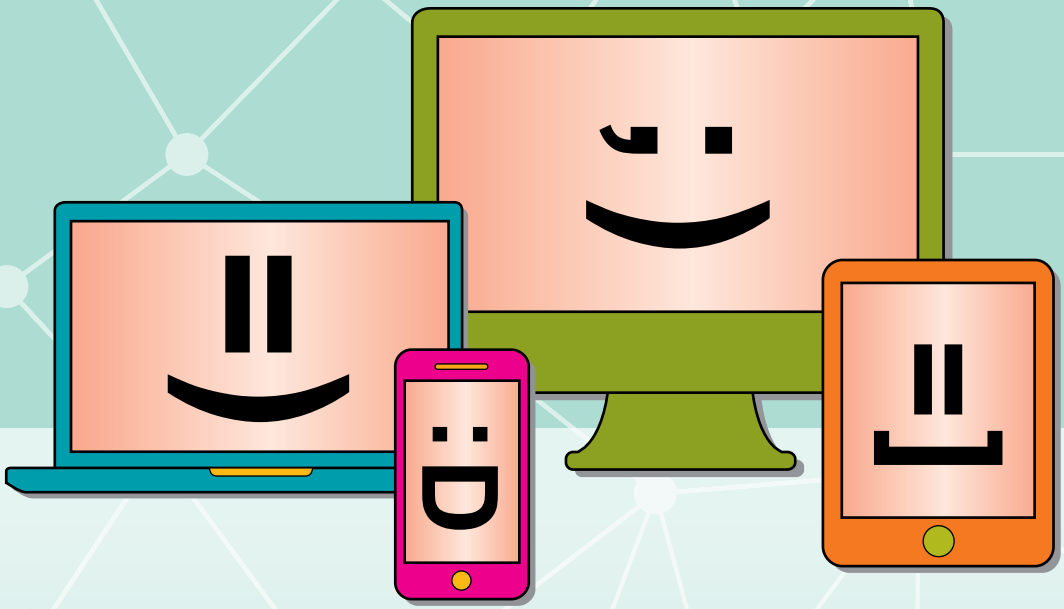
NAVEGAR COM SEGURANÇA:

por uma internet mais segura, ética e responsável



2017

4ª edição

Ministério Público do Estado de Minas Gerais

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS

Coordenadoria Estadual de Combate aos Crimes Cibernéticos – COECIBER

Responsável

Christianne Cotrim Assad Bensoussan – Promotora de Justiça e Coordenadora do COECIBER

Texto

Christianne Cotrim Assad Bensoussan
Flavianne Lenimar Vieira Brandão Silva
Hérika Alonso Cicarelli Fonseca
Hugo Vieira
Luiz Claudio Ferreira do Nascimento
Marcelle Mascarenhas Teixeira
Maria Isabel Lara Oliveira
Nairo de Assis Barbosa Junior
Nathalia Danielle Ribeiro de Oliveira
Paulo Leonardo Benício Praxedes
Rafael Coutinho Camargos
Riany Alves de Freitas
Ricardo Gonçalves Pessoa Leite

Superintendência de Comunicação Integrada

Revisão: Ana Paula Rocha, Jadhe Gonçalves e Marco Melo
Projeto de identidade visual: Fabrício Passos
Projeto gráfico e diagramação: Rúbia Guimarães

PGA Plano Geral de Atuação | Finalístico | 2017

Projeto: **Internet Segura**

MPMG
Ministério Público
do Estado de Minas Gerais

O Ministério Público defende os interesses da sociedade e tem como função zelar pela aplicação da lei, atuando nas áreas Cível, Criminal e de Defesa do Cidadão por meio das diversas Promotorias de Justiça.

No Ministério Público de Minas Gerais (MPMG), a Coordenadoria Estadual de Combate aos Crimes Cibernéticos é o órgão que tem a missão de combater os crimes cibernéticos (ou telemáticos). Com o objetivo de alertar sobre crimes cometidos na internet e orientar sobre como se proteger nos ambientes virtuais, o Órgão promove, nas escolas, palestras voltadas a alunos, pais e professores para conscientização dessas pessoas a respeito dos perigos existentes na rede mundial de computadores. Além disso, produz e distribui materiais informativos.

Esta edição da cartilha **Navegar com segurança: protegendo seus filhos da pedofilia e da pornografia infantojuvenil,** reformulada e atualizada, é fruto dos esforços conjugados da equipe integrante da Coordenadoria Estadual de Combate aos Crimes Cibernéticos. Desde a sua primeira edição, vem tratando o tema com o objetivo de construir uma rica abordagem sobre o uso adequado da internet. Como o ambiente virtual passa por diversas transformações, é constante a necessidade de atualização deste material. Agradecemos, portanto, as contribuições das equipes responsáveis pelas produções anteriores, sem as quais esta Cartilha não teria a força necessária para a realização de novas edições.

como anda sua VIDA VIRTUAL?

A INTERNET CONECTOU O MUNDO.

Os conceitos de comunicação a distância foram profundamente modificados. Além de o mundo inteiro estar o tempo todo conectado, a comunicação entre pessoas a longa distância deixou de ser um problema; notícias são compartilhadas instantaneamente a nível global; uma fonte inesgotável de informações está constantemente disponível para estudantes e curiosos; instituições, empresas, governos, entre outros, operam suas atividades em meio virtual. Esses são alguns entre tantos outros pontos positivos da rede mundial de computadores.

Entretanto, há também a parte negativa da rede. É muito importante conhecer e compreender as ações nocivas realizadas nesse ambiente. Então, antes de falar desse outro lado, é preciso pensar:

com que objetivos se acessa a internet?

É para se comunicar? Para se informar, trabalhar, estudar, jogar, pesquisar, ler notícias, fazer amigos

ou apenas para se desligar do mundo real e conectar-se ao mundo virtual em busca de um espaço aberto e livre de qualquer censura por parte da sociedade?

Quaisquer que sejam os motivos para acessar a internet,
precisamos entender que não existe uma vida virtual.
Existe apenas a vida real, que passou a ser exposta e observada no mundo virtual,
principalmente através das redes sociais.

Assim como na vida real, na internet temos DIREITOS E DEVERES.

As suas ações no ambiente virtual sempre refletirão em sua vida real, em seu dia a dia,
sejam elas positivas ou negativas.

FIQUE BEM ATENTO!

Tudo o que acontece na internet reflete o comportamento das pessoas que a utilizam, e os ambientes virtuais estão cheios de perfis falsos e pessoas mal-intencionadas.

Diariamente, têm-se notícias de pessoas enfrentando sérios problemas na internet.

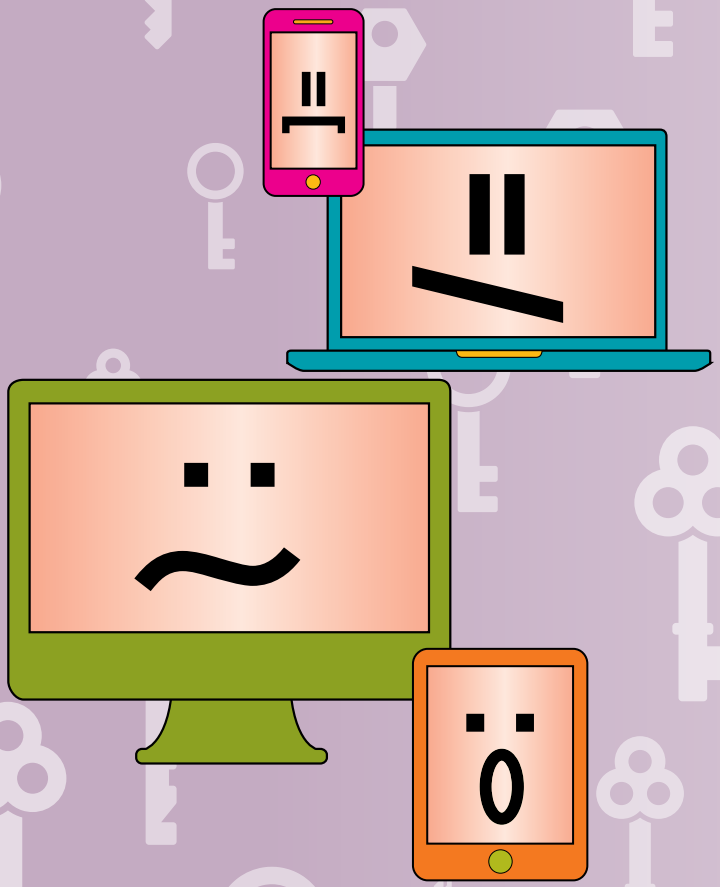
PORNOGRAFIA INFANTIL
***CYBERBULLYING* - ESTELIONATO**
EXTORSÃO - CALÚNIA

são apenas alguns deles.

Não se iluda:

eles podem acontecer com você, com sua família, com seus amigos, com seus filhos.

e como anda SUA PRIVACIDADE?



A PRIVACIDADE

pode ser entendida como o direito de cada indivíduo de manter-se reservado e de controlar as informações sobre seu modo de vida, suas ideias, suas relações familiares e afetivas, seus hábitos, sua intimidade.

A privacidade é um direito universal e também garantido pela nossa Constituição.

O Marco Civil da Internet,

lei aprovada em 2014, estabelece normas para a proteção da privacidade, seja em relação à guarda e ao tratamento de registros, dados pessoais ou comunicações por *sites* ou empresas que prestem serviços de acesso à internet, seja em relação à forma como essas informações devem ser disponibilizadas ao cidadão.

É importante cuidar da sua privacidade e da sua vida íntima, assim como da de sua família e de seus amigos.

VEJA A SEGUIR ALGUNS CUIDADOS SIMPLES QUE VOCÊ PODE TOMAR:

SEMPRE QUE ALGUÉM

solicitar seus dados ou quando você precisar preencher algum cadastro, reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso a suas informações.

PROCURE SEMPRE

se informar sobre os termos de usos e políticas de privacidade dos serviços que você usa na internet.

CRIANÇAS DEVEM

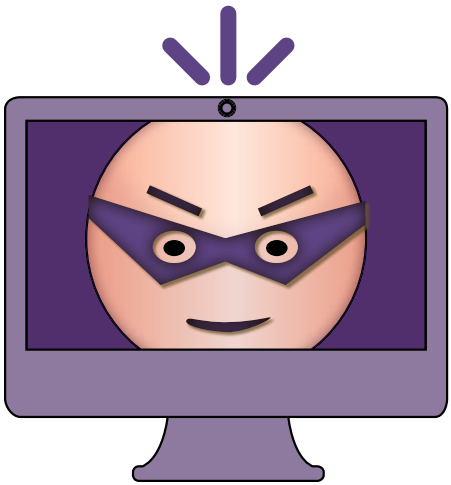
acessar serviços, jogos e redes sociais e assistir a vídeos adequados à sua idade. Devem ainda ser monitoradas pelos pais ou responsáveis. Existem maneiras de monitorar ou bloquear conteúdos impróprios para menores de idade. Fique atento à publicidade infantil.

SEJA CUIDADOSO

ao divulgar informações em redes sociais. Endereços, telefones e números de documentos nunca devem ser informados nesses meios. Publicar fotos pessoais e de familiares as quais facilitem a identificação de lugares frequentados por vocês, assim como divulgar sua localização geográfica, pode ajudar criminosos e pessoas de má-fé a identificar a sua rotina e seus hábitos diários.

NUNCA COMPARTILHE

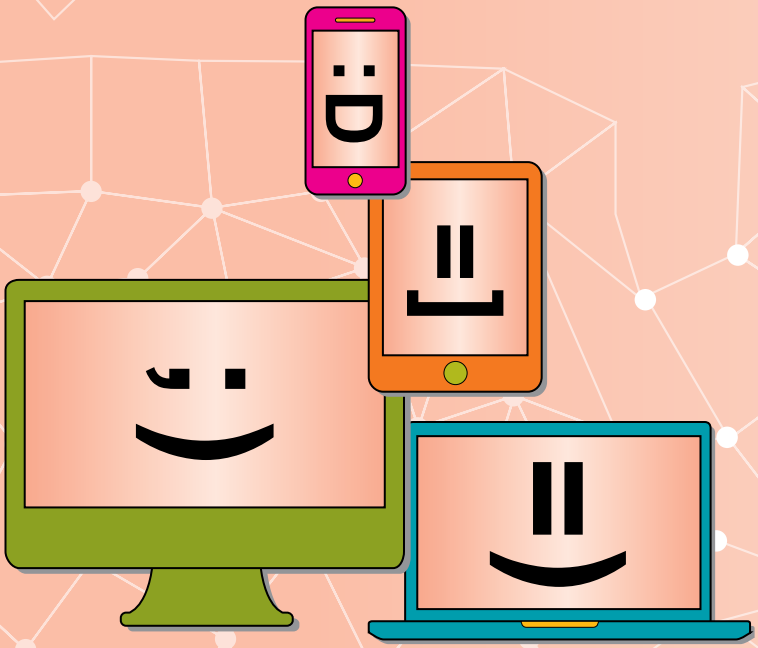
suas senhas pessoais.



NÃO ABRA SUA *WEBCAM*

para desconhecidos: ela pode colocar um criminoso dentro da sua casa.

como podemos nos cuidar nas REDES SOCIAIS?



As redes sociais são espaços para encontro de pessoas e compartilhamento de mensagens de texto, mensagens de voz, imagens, vídeos e fotos. Hoje também são muito utilizadas em relações comerciais e institucionais. A cada ano surgem novas redes para atrair e disputar a atenção de quem gosta de socializar-se virtualmente.

É preciso ser cuidadoso e monitorar crianças e adolescentes para o uso correto e mais seguro das redes. A idade mínima de acesso pode variar conforme o *site* de relacionamento. RESPEITE sempre esse limite de idade para cadastrar-se nas redes sociais.

Ao criar um perfil nas redes sociais, fique atento às informações que vai fornecer (por exemplo, preferências pessoais), bem como à configuração da privacidade do conteúdo publicado, para que o acesso às suas informações e postagens seja compartilhado apenas com as pessoas e grupos com que você pretende se relacionar.

Antes de adicionar um desconhecido às suas redes sociais, analise bem as publicações dele e os amigos que vocês têm em comum. As redes sociais estão cheias de perfis falsos e de pessoas mal-intencionadas.

AMIGO NÃO É QUALQUER UM!

O que importa é a qualidade e não a quantidade de amigos que uma pessoa possui. Tenha muito cuidado com estranhos.

CRIE SENHAS "FORTES".
Mescle números, letras e outros caracteres.

NÃO COMPARTILHE SUA SENHA COM NINGUÉM.

NÃO FIQUE "LOGADO"
o tempo todo.

CLIQUE EM "SAIR"
sempre que deixar de usar a rede.

Seja cuidadoso com as informações que você vai publicar no seu perfil.

As redes sociais podem coletar e gravar informações, como seu histórico de pesquisa, enquanto você navega na internet, por exemplo, quando você publica uma atualização de *status*, carrega uma foto, comenta sobre a história de um amigo, adiciona alguém, curte uma página, navega em um *site* a partir da rede social, faz *check-in* em um local ou quando importa a lista de contatos de outra rede ou do seu *e-mail*. E mais, acredite: sua localização em cada postagem pode ser gravada.

Não compartilhe fotos, informações pessoais ou sua localização com pessoas desconhecidas. Evite divulgar endereços e locais onde frequenta, mora ou estuda.

O que você compartilha com seus amigos não fica só entre vocês. Informações pessoais tornam-se públicas e o que você divulga nas redes dificilmente será removido depois. Se você tem algo íntimo para dizer a alguém, fale pessoalmente ou use o telefone.

Então, lembre-se: mesmo quando você toma todos os cuidados, CAIU NA REDE É PÚBLICO!

Devemos respeitar sempre a diversidade de culturas e opiniões.

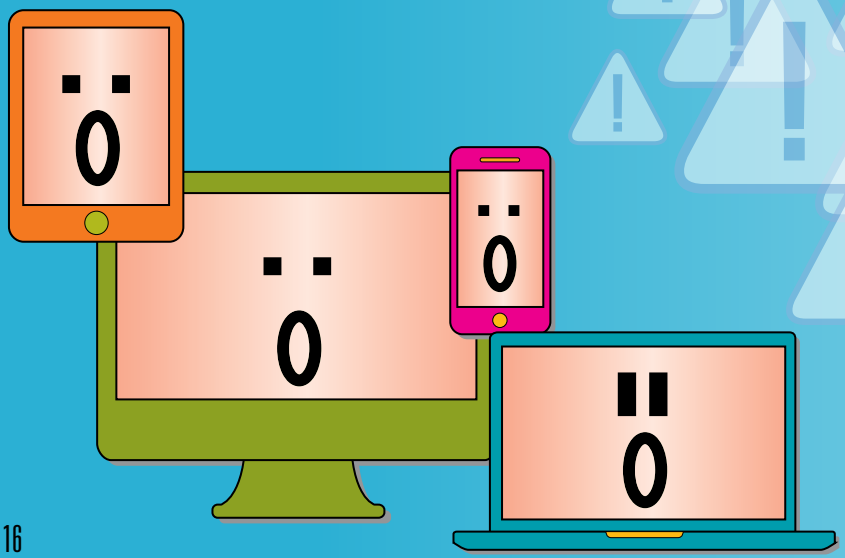
Não podemos NUNCA disseminar preconceitos de cor, gênero, religião, orientação sexual, origem social ou de qualquer outro tipo.

Não publique conteúdos ofensivos. Não responda a provocações nem ofenda outras pessoas. Devemos fazer um uso seguro, ético e responsável das ferramentas que a internet oferece.

CONTEÚDOS OFENSIVOS E IMPRÓPRIOS PODEM E DEVEM SER DENUNCIADOS PELOS USUÁRIOS.

Nós também somos o que curtimos e compartilhamos.

quais são os principais PERIGOS NA INTERNET?



CYBERBULLYING

A Lei nº 13.185/15 instituiu o Programa de Combate à Intimidação Sistemática (***bullying***), descrevendo as formas de ocorrência, os objetivos e as consequências dos atos característicos do ***bullying*** e ***cyberbullying***.

Bullying

é uma palavra de origem inglesa, derivada do verbo ***to bully*** (ameaçar, amedrontar, intimidar).

É considerado *bullying* todo ato de

violência física ou psicológica,

intencional e repetitivo

praticado por indivíduo ou grupo,

contra uma ou mais pessoas,

causando dor e angústia,

dentro de uma relação desigual de poder,

intimidando a vítima.

É um problema universal que cresce a cada dia, principalmente no ambiente escolar, devendo ser cotidianamente combatido.

OFENDER, HUMILHAR, AMEAÇAR OUTRAS PESSOAS

através de fotos, vídeos ou comentários violentos, assim como

CAUSAR VERGONHA, INTIMIDAÇÃO E MEDO,

são formas de *cyberbullying*.

QUALQUER UM,

inclusive adultos, pode se tornar vítima desses atos.

O *CYBERBULLYING*

é uma das formas mais agressivas de *bullying* que ganha cada vez mais espaço. A vítima do *cyberbullying* sofre com as agressões e repetidos ataques de diferentes naturezas dentro do mundo virtual, seja por redes sociais ou qualquer outro veículo tecnológico de informação, o que pode levar a sérios transtornos psicológicos e físicos. O mundo virtual tornou-se um campo fértil para a prática do *bullying*.

Por um lado, devido ao alcance e à velocidade das ofensas e, por outro, à possibilidade de o agressor se manter no anonimato, utilizando nomes falsos. Os efeitos do *cyberbullying* podem ganhar dimensões incalculáveis.

Se existe uma situação em que somente alguns se divertem e outros são maltratados e sofrem, o problema é sério e precisa de intervenção.

Cyberbullying
NÃO É BRINCADEIRA.

O *bulllying* e o *cyberbulling* são modos de demonstrar poder. Porém, quando esses atos de violência são cometidos por uma criança ou adolescente, podem ser um sinal de que os agressores também estejam passando por problemas e dificuldades e expressando seu sofrimento através da violência.

Se você está sofrendo ou conhece alguém que sofre com atos de violência, psicológica ou física, com o fim de denegrir e humilhar,

não tenha medo, encoraje-se! DENUNCIE.

Crianças e adolescentes:

contem o que está acontecendo para seus pais ou alguém que seja de sua confiança.

Não respondam a mensagens ofensivas

nem as excluam.Imagens e outros arquivos também não devem ser apagados.

Diálogo e orientação

são sempre o melhor caminho. Os pais ou responsáveis e as escolas devem ajudar e podem ser responsabilizados se forem negligentes.

Não deixem o problema se agravar.

Busquem ajuda. Procurem o Ministério Público, o Conselho Tutelar ou a Delegacia de Polícia mais próxima de sua cidade. Certas situações podem se desdobrar em tragédias.

PORNOGRAFIA INFANTOJUVENIL

Certas pessoas podem tentar

seduzir, convencer e chantagear

crianças ou adolescentes, com o objetivo de

obter imagens eróticas e sexuais.

Essas pessoas podem fazer parte de redes criminosas que usam essas imagens para produzir material pornográfico para pedófilos*.

***mulheres e homens adultos que têm atração por crianças e adolescentes**

Nessa situação, pessoas adultas se passam por crianças ou adolescentes, usam uma linguagem compatível com a idade da pessoa com quem conversam e falam de assuntos que interessam ao universo infantojuvenil. No geral, são amáveis e fazem muitos elogios com a intenção de ganhar a confiança de meninos e meninas e conseguir informações que facilitem a obtenção de fotos, vídeos e outros materiais para uso criminoso.

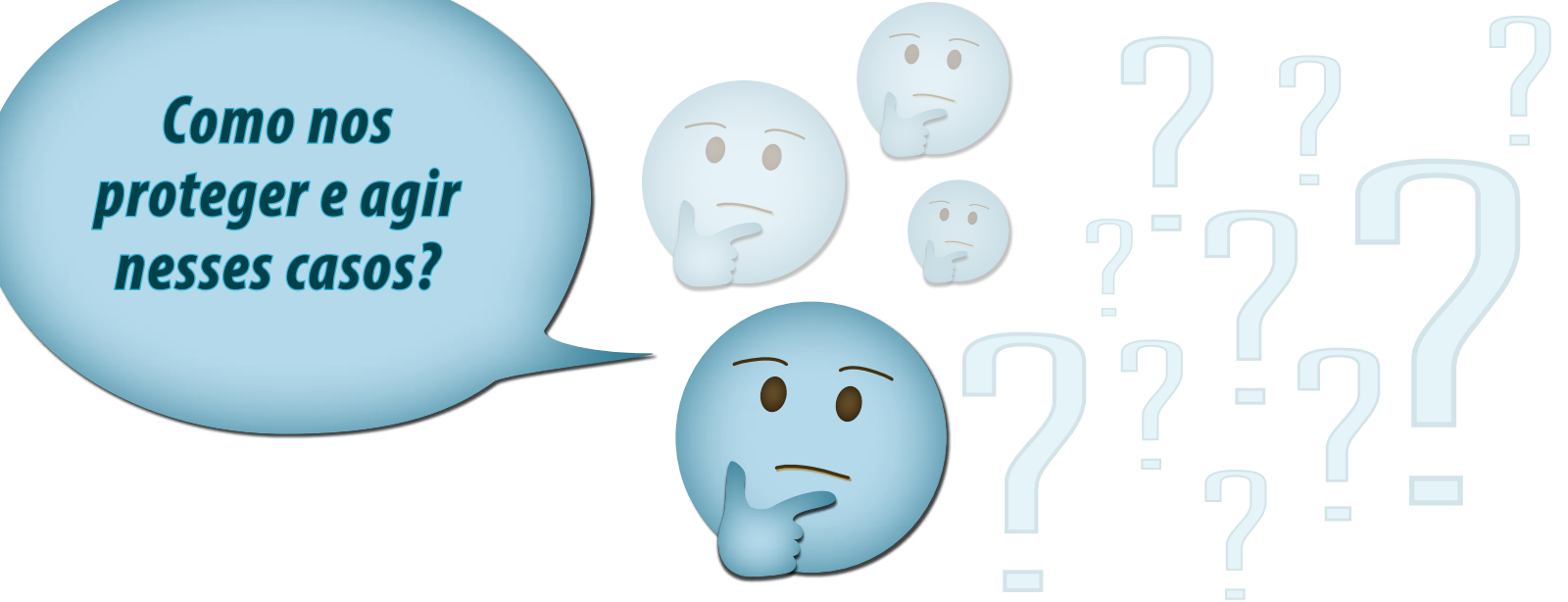
O contato pode acontecer nas redes sociais, nos aplicativos de mensagens, nas salas de bate-papo, em jogos* on-line *ou em qualquer outro ambiente virtual de relacionamento.

Geralmente, os criminosos solicitam a ativação da *webcam* ou da câmera do celular para que sejam capturadas fotos e vídeos da vítima. Assim, manipulam as crianças e adolescentes para obrigá-las a fazer o que não querem e a enviar conteúdos pornográficos.

É comum que essas pessoas façam com que crianças e adolescentes sintam-se culpados pela situação, forçando-os a não contar para ninguém.

Os criminosos podem tentar marcar encontros pessoais com crianças e adolescentes, podendo, nos piores casos, terminar em

SEQUESTRO E ABUSO SEXUAL DAS VÍTIMAS.



EVITE USAR A *WEBCAM*,

transmitir vídeos e fotos ou fazer ligações ao vivo com estranhos. Sua imagem pode ser manipulada e montada em situações humilhantes e, então, divulgada no ambiente virtual.

FAÇA GRAVAÇÕES E SALVE MENSAGENS E FOTOS

quando houver ameaças verbais ou por meio de imagens violentas. Bloqueie o contato dos agressores no celular e em todas as redes de relacionamento.

LEMBRE-SE:

crianças e adolescentes precisam do

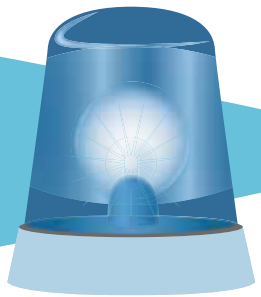
apoio e da confiança dos pais e responsáveis.

DENUNCIE SEMPRE.

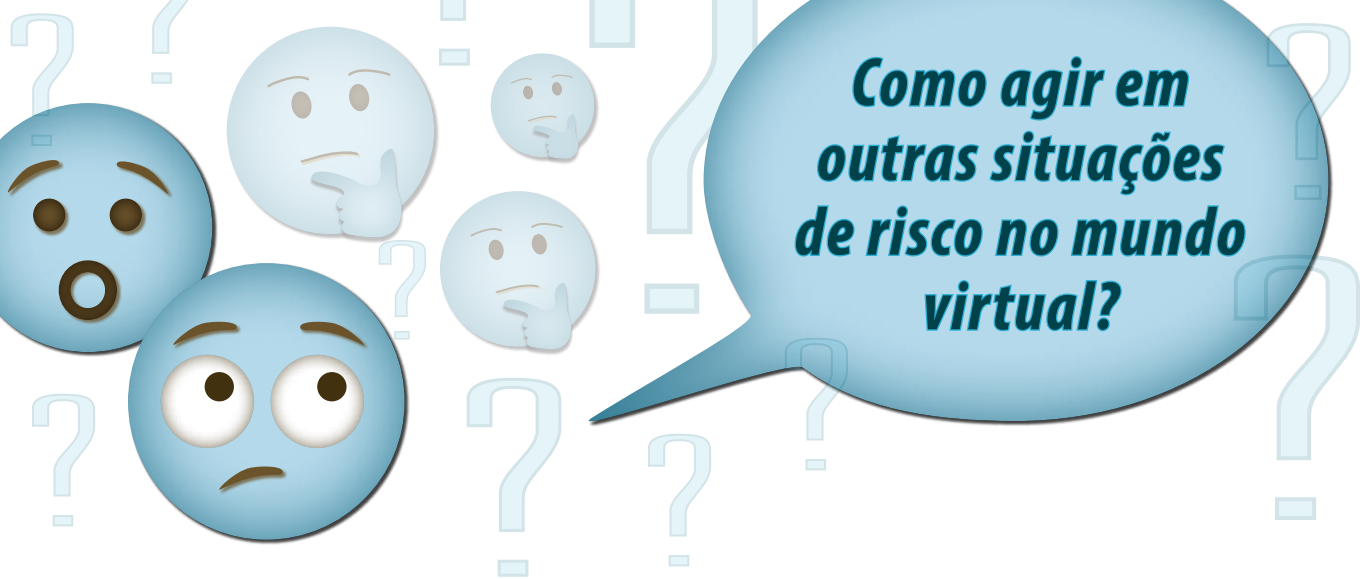
Se está acontecendo algo assim com você ou com seus amigos, não tenha medo. Conte para seus pais ou para alguém de confiança. Você também pode buscar ajuda no Ministério Público, no Conselho Tutelar, na delegacia de polícia mais próxima, no Disque 100 e no Disque 190.

Pornografia infantojuvenil

É CRIME!



Se você detectar um conteúdo desse tipo na internet, denuncie.



FIQUE ALERTA!

Mesmo tomando todas as precauções, os bloqueios de acesso podem ser "derrubados" por pessoas mal-intencionadas e criminosas.

Seus dados podem ser roubados e usados para ofender ou chantagear.

Criminosos podem criar perfis falsos e robôs para envio de mensagens automáticas.

Caso você tenha o perfil invadido, clonado ou sofra agressão nas redes, faça o seguinte:

- Dê um *printscreen* das telas ou fotografe-as. Em ambos os casos, fique atento para que a identificação do agressor fique clara e legível. É importante que a URL (endereço da página na internet) também fique claramente identificável.

- Imprima tudo o que possa servir como prova (conteúdo da comunidade, mensagem ou imagem ofensiva, página inicial do usuário responsável por aquele conteúdo).

Nunca exclua sua conta no Facebook!

- Ao invés disso, use o recurso "desativar sua conta". Dessa maneira ela fica indisponível para todos na internet, mas preserva o conteúdo até então armazenado.

- Faça um *backup* (cópia) completo de seu perfil e apresente à autoridade policial. Nele existem informações importantes que podem auxiliar na identificação do(s) criminoso(s).

No WhatsApp,

- se você participar de algum grupo suspeito ou ofensivo, envie a conversa para seu *e-mail*. Isso também vale para conversas privadas cujo conteúdo seja agressivo.

- É importante que os números dos telefones dos envolvidos estejam legíveis e completos.

A divulgação de imagens e vídeos íntimos como forma de humilhação pública ou punição e com o objetivo de se vingar, expor a intimidade, macular a reputação e extorquir é mais comum do que imaginamos.
E não acontece só com adolescentes.

PORNOGRAFIA DE REVANCHE

Também denominada pornografia de vingança, pornografia não consensual ou *revenge porn*.

Quem são as vítimas?

As vítimas são, em sua maioria, mulheres que tiveram suas imagens íntimas divulgadas por uma pessoa com a qual mantiveram relacionamento amoroso, eventual ou não.

Quando a vítima é mulher, na maioria das vezes,
o intuito da divulgação é desmoralizar e punir, sem que o agressor exija ou obtenha qualquer vantagem com isso.

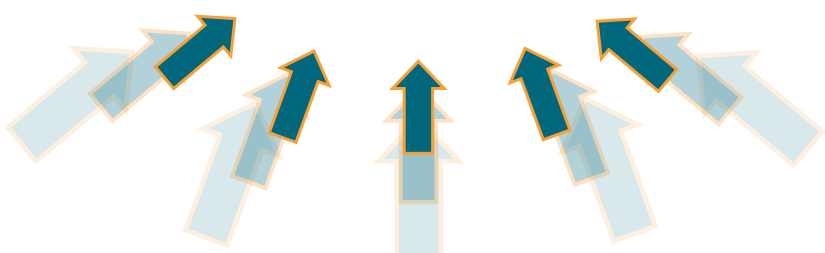
Quando a vítima é homem, na maioria das vezes,
a ameaça de divulgação é precedida de extorsão.

A pornografia de revanche pode ser considerada uma nova expressão da violência de gênero.

A ameaça de divulgação de imagens e vídeos íntimos como modo de extorsão atinge homens e mulheres e é um fenômeno mundialmente conhecido como *sextortion*.

Fotos ou vídeos podem ser produzidos com ou sem consentimento da vítima.

Imagens podem ser capturadas de diversas formas, inclusive através do uso da *webcam*. Também podem ser obtidas através de invasão de computadores e dispositivos.



Não basta ter cuidado com o que publicamos na internet e nas mídias sociais.

Muitas vezes, o simples fato de curtir, compartilhar ou retweetar uma imagem ou informação pode prejudicar muitas pessoas.

Esse tipo de interação já arruinou muitas vidas, assim como levou a diversas condenações na Justiça.

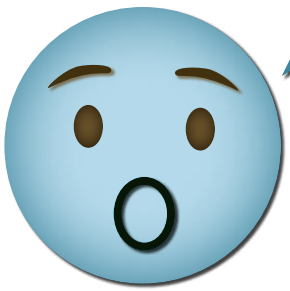
Então, pense antes de clicar:

isso vai valer a pena?

Nós também somos aquilo que

CURTIMOS E COMPARTILHAMOS.

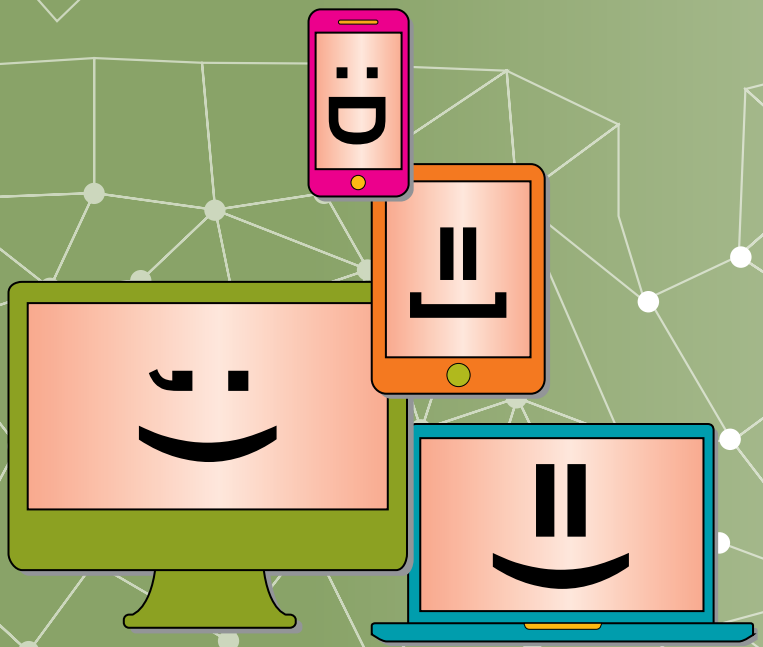
Colabore para um ambiente mais respeitoso e ético na internet. Seja responsável.



Se você identificar conteúdos de cunho racista, preconceituoso, discriminatório, que incitem a intolerância ou que envolvam cenas de violências contra crianças e adolescentes, não se cale!

DENUNCIE PÁGINAS E PERFIS QUE PRATIQUEM CRIMES NA INTERNET.

outras formas de interação e acesso À INTERNET

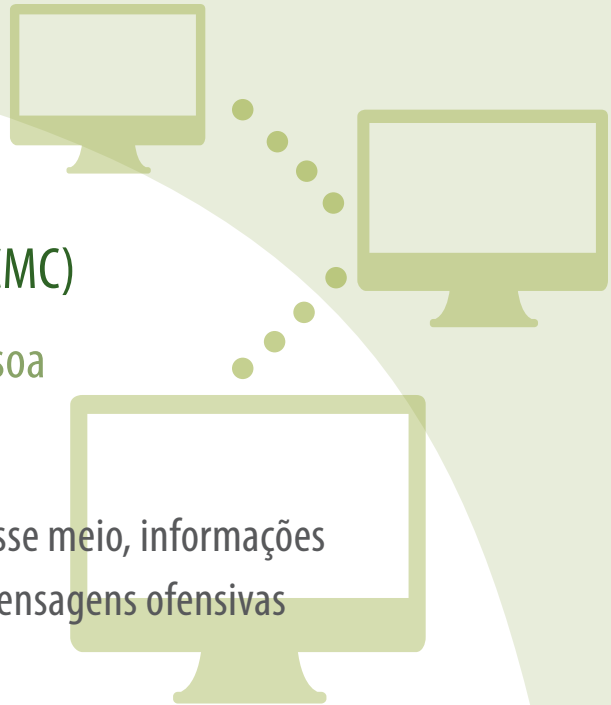


Dicas técnicas

MENSAGENS INSTANTÂNEAS

Comunicação mediada por computador (CMC)

Serviço de conversação *on-line* com outra pessoa também conectada à internet.



Assim como nas redes sociais, não transmita, por esse meio, informações pessoais, fotos e outros arquivos para estranhos. Mensagens ofensivas e crimes também podem ser cometidos via CMC.

Pessoas mal-intencionadas podem simular-se conhecidas, pedir depósitos em dinheiro e aplicar outros golpes.

Links com programas maliciosos (vírus) podem ser enviados.
Não abra *links* suspeitos ou arquivos desconhecidos.

Se tiver conhecimento de infração cometida por meio de mensagens instantâneas, salve e imprima o conteúdo das mensagens, além das informações sobre o interlocutor (números identificadores, apelidos ou *e-mail*), anotando a data e o horário da comunicação. De posse de todas essas informações, procure uma delegacia especializada, a delegacia de polícia mais próxima ou o Ministério Público.

WEBSITES E COMÉRCIO ELETRÔNICO (*e-commerce*)

Website, ou simplesmente *site*, é um conjunto de informações que podem ser acessadas através da digitação de um endereço de internet em um navegador e apresenta os mais diversos conteúdos.

Já *sites* de *e-commerce* são espaços virtuaisde comercialização de produtos e serviços.

Fique atento:

- Algumas páginas na internet podem ser falsas. Tome cuidado ao fazer cadastros e colocar informações pessoais.
- Monitore crianças e adolescentes para que não acessem páginas com conteúdo pornográfico e impróprio para a idade deles.
- Faça *download* de programas e aplicativos diretamente do *site* do fabricante.

- Sempre use uma conexão segura, principalmente ao transmitir dados sensíveis, como se faz nos acessos a *sites* de *internet banking* e de comércio eletrônico.

- Os endereços de *sites* com conexão segura começam com <https://>. O desenho de um cadeado fechado é mostrado na barra de endereço e, ao clicar sobre ele, detalhes sobre a conexão e sobre o certificado digital em uso são exibidos.

- Principalmente em caso de compras, dê preferência a *sites* com endereço final <.com.br>. Domínios cadastrados no estrangeiro – como nos endereços de final <.com> – dificultam a ação da polícia.

Dicas para compras mais seguras na internet:

NÃO COMPRE

em *sites* de procedência desconhecida. Verifique se pessoas de sua confiança já compraram naquele *website*. Em caso positivo, confira também se receberam o produto e se ele foi entregue no prazo prometido. Além disso, consulte se há reclamações sobre o vendedor no endereço <www.reclameaqui.com.br>.

CONSULTE

o *site* de vendas no <www.registro.br> e verifique os dados completos de quem registrou o domínio e o CNPJ, assim como o endereço e o telefone de contato da empresa responsável. Cheque também se os dados estão corretos. Desconfie quando um *site* fornecer apenas telefone celular como forma de contato.

CONFIRME

se o *site* é seguro. Todos aqueles que oferecem condições seguras de acesso começam com <https://> e possuem a imagem de um cadeado fechado. Isso indica que a loja virtual trabalha com certificado de segurança.

VERIFIQUE

a política de privacidade da loja virtual. Saiba qual o compromisso do vendedor em relação à manipulação dos dados que você informa.

EVITE

colocar sua senha ou seus dados pessoais em *links* fornecidos por *e-mails*, ainda que aparentemente eles tenham sido enviados pelo *site* no qual você se cadastrou.

CRIE

uma de *e-mail* específica para compras na internet.

OFEREÇA

o mínimo de informações para completar a transação. Evite acrescentar dados que não tenham relação alguma com a concretização do negócio.

VERIFIQUE

as características do produto, condições de entrega, tarifas de envio, formas de pagamento e condições de troca.

CONFIRME

na página do fabricante se as características do produto condizem com as fornecidas pelo *site* do vendedor.

DESCONFIE

de propostas muito boas, produtos milagrosos ou de preço muito inferior ao de mercado.

REGISTRE

toda a negociação e transação, como *e-mails*, anúncios, telas do *site* de compra e toda a comunicação estabelecida com a loja.

Caso seja vítima de estelionato ou se tiver conhecimento de infração cometida num *site* da internet, capture as páginas (faça um *printscreen* ou fotografe a tela do computador) e reúna todos os registros e informações, como contas bancárias envolvidas na transação, mensagens enviadas e recebidas, boletos bancários e qualquer outra informação. Procure a delegacia especializada em crimes cibernéticos, a delegacia de polícia mais próxima ou o Ministério Público.

BLOGS

Blog é um *site* que permite a atualização rápida de conteúdo a partir de acréscimos de artigos ou *posts*. As postagens, em geral, ficam organizadas da mais recente para a mais antiga. Podem ser escritas por uma ou várias pessoas, de acordo com a política do *blog*.

Fique atento:

- O anonimato é proibido no Brasil, por isso todo conteúdo deve ter o registro que identifique o responsável.
- Assim como nas redes sociais, seja educado, ético e responsável. Não publique conteúdos ofensivos e difamatórios, que ridicularizem outras pessoas.
- Não publique informações pessoais ou relacionadas a sua rotina diária ou a de sua família.
- Verifique a veracidade das informações antes de publicá-las.
- Somente utilize imagens de outras pessoas se o uso delas for previamente autorizado.
- Respeite os direitos autorais na internet, citando a fonte de referência do conteúdo utilizado (textos e/ou imagens).

E-MAIL OU CORREIO ELETRÔNICO

E-mail é um sistema eletrônico de comunicação para envio de mensagens escritas. O correio eletrônico é anterior ao surgimento da internet. De fato, os sistemas de *e-mail* foram uma ferramenta fundamental para a criação da rede mundial de computadores. Além do texto, suportam o envio de vídeos, fotos e arquivos diversos.

Fique atento:

- Crie uma conta de *e-mail* própria para assuntos pessoais, uma para assuntos profissionais e outra para compras na internet.

- Seja muito cuidadoso com *e-mails* de pessoas ou origem desconhecidas. Muitas delas podem ser *spam*, que são mensagens enviadas em massa para múltiplas pessoas e que normalmente possuem propagandas indesejadas, informações falsas, códigos maliciosos e vírus, podendo danificar seus aparelhos, arquivos e ainda capturar informações e senhas.

- Configure seu programa de leitor de *e-mails* para que imagens que não estejam no corpo do texto não exibir sejam exibidas automaticamente.

- As mensagens de *e-mail* são um poderoso veículo de propagação de vírus, sobretudo através de arquivos anexos. Por isso recomenda-se nunca abrir arquivos desconhecidos ou suspeitos ou baixar um arquivo do tipo <.exe> (executáveis). Não clique em *links* desconhecidos. Não acredite em *e-mails* que induzam à instalação ou execução de programas, assim como ao preenchimento de informações pessoais.

- Verifique as fraudes registradas, comumente recebidas por *e-mail*, no Centro de Atendimento a Incidentes de Segurança (CAIS): <http://www.rnp.br/cais/fraudes.php>.

- Instituições governamentais, bancos e empresas sérias e idôneas não costumam enviar *e-mails* solicitando informações dos cidadãos, principalmente senhas, ou pedindo para clicar em *links*. Desconfie sempre desse tipo de mensagem.

- Seja sempre cuidadoso com crianças que utilizam a comunicação via *e-mail*, pois elas podem receber conteúdos impróprios.

***Lembre-se: use uma conexão segura sempre que estiver acessando seus* e-mails.**

SALAS DE BATE-PAPO (*CHATS*)

São espaços virtuais que possibilitam conversas simultâneas entre diversas pessoas.

Fique atento:

- Não há controle de acesso, portanto qualquer pessoa pode entrar nas salas de bate-papo, bastando criar um apelido.

- Raramente se sabe ao certo quem está participando da conversa. Nesses ambientes, pessoas mal-intencionadas podem tentar obter informações pessoais para usá-las indevidamente. Então, não poste fotos ou informações pessoais.

- O conteúdo das conversas pode ser impróprio para menores. Não permita que crianças e adolescentes acessem as salas de bate-papo sem o acompanhamento devido, por serem ambientes propícios a trocas de mensagens de teor ofensivo e pornográfico.

- As mensagens podem trazer *links* e anexos que danificam o computador ou enviam informações (como senhas) a pessoas desconhecidas e mal-intencionadas na rede.

JOGOS *ON-LINE*

São jogos que necessitam de uma conexão de internet para que o usuário possa participar e interagir com outros jogadores, seja pelo computador, pelos consoles (*video games*) ou pelos *smartphones* e *tablets*.

Fique atento:

- Preste bastante atenção às permissões que são solicitadas ao baixar jogos nos *smartphones* e *tablets*. Instale os jogos somente a partir do *site* do fabricante ou das lojas oficiais.

- Baixar jogos em *sites* não confiáveis ou que contenham cópias não autorizadas, além de ser tipificado como crime (art. 12 da Lei nº 9.609/1998), pode danificar seu computador e colocar em risco todas as informações nele contidas.

- Códigos maliciosos podem ser espalhados por meio de cópias falsas de jogos *on-line*, possibilitando o acesso não autorizado a informações como senhas e dados dos usuários.

- Nem todos que estão jogando são bem-intencionados. Existem criminosos que se aproveitam de fóruns *on-line* sobre jogos para conseguir informações pessoais de seus participantes, como telefone e endereço, usando-as, posteriormente, para cometer crimes reais e virtuais.

- Evite o uso de senhas óbvias ou com informações pessoais que sejam fáceis de serem desvendadas.

- Proteja seu computador, instale um bom antivírus e mantenha os programas atualizados com as últimas correções de segurança. Esses cuidados também valem para dispositivos móveis, pois eles também estão propícios a esse tipo de ameaça.

- Crianças e adolescentes devem ser monitorados no uso dos jogos, pois cada um delesl possui características diferentes e são recomendados para faixas etárias específicas.

NOTEBOOKS, TABLETS E *SMARTPHONES*

Smartphones, *tablets* e *notebooks* podem ser importantes aliados em sala de aula e no trabalho. Além de permitirem diversão e lazer, esses aparelhos com acesso à internet são instrumentos práticos e eficientes para reduzir o esforço e aumentar o aproveitamento em cursos e atividades profissionais.

Fique atento:

- Antes de utilizar esses recursos, é importante que você conheça as regras de uso desses aparelhos nos mais variados ambientes. Procure saber qual a política de uso de tecnologias móveis no ambiente escolar e no trabalho.

- Aparelhos portáteis podem armazenar conta de *e-mail*, senhas, fotos, arquivos, entre outras informações pessoais, e a chance de perder esses equipamentos é bem maior. Em caso de perda ou furto, suas informações podem cair nas mãos de pessoas mal-intencionadas.

Cuidados a tomar:

- Assim como em um computador, utilize e mantenha atualizados mecanismos de segurança, como programa antimalware e *firewall* pessoal.

- Proteja com senha os aparelhos portáteis e os aplicativos. Tenha cuidado com as informações neles guardadas.

- Configure a geolocalização do aparelho e, se possível, o acesso remoto a ele, possibilitando apagar todos os seus dados e informações em caso de necessidade.

- Não destrua seu dispositivo! Esta é uma atitude não aconselhada, pois pode eliminar provas e evidências importantes para identificar alguém mal- intencionado.

- Cuidado com fotos e vídeos íntimos. Sempre há a chance de que esses arquivos sejam disseminados e usados indevidamente, sem sua autorização.

SENHAS

Uma senha serve para assegurar que você é realmente quem diz ser e que possui o direito de acessar o recurso desejado. É um dos principais mecanismos de autenticação usados na internet devido, principalmente, à simplicidade que possui.

Fique atento:

- Senhas são pessoais e intransferíveis e não devem ser compartilhadas.
- Senhas fracas podem ser facilmente descobertas. Utilize senhas longas, entre 8 e 12 caracteres. Procure mesclar letras maiúsculas e minúsculas, números e caracteres especiais. Evite sequências ou caracteres repetidos.
- Troque suas senhas regularmente ou sempre que achar necessário.
- Não use a mesma senha para todos os serviços que acessa.
- Ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas.
- Certifique-se de que não está sendo observado ao digitar as suas senhas.

WI-FI

Tecnologia de comunicação que não faz uso de cabos ou fios e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.
O roteador, ou *modem*, é o dispositivo que as operadoras disponibilizam para acesso à internet, seja a cabo ou sem fio.

Fique atento:

- Esse tipo de aparelho é muito vulnerável e pouquíssimas pessoas se preocupam em trocar a senha-padrão a ele atribuída.

- Crie uma senha de acesso muito forte para ele. Caso a esqueça, basta a "resetar" o roteador e criar uma nova senha. O importante é deixar o dispositivo sempre bem protegido.

- Redes *wi-fi* abertas, sem proteção, podem ser um grande risco para os internautas. Elas são o principal alvo de criminosos virtuais que, ao utilizarem uma rede em nome de outra pessoa, são dificilmente descobertos.

- Desligue seu *modem* quando não mais estiver utilizando sua rede.

DENUNCIE OS CRIMES VIRTUAIS!

Caso seja vítima de algum desses crimes, procure a delegacia especializada em crimes cibernéticos, a delegacia de polícia mais próxima ou o Ministério Público.

Clique aqui e acesse a página de crimes cibernéticos do Ministério Público de Minas Gerais, onde denúncias podem ser feitas pelo *link*: **Para enviar uma denúncia, realizar complementações e consultas clique aqui.**

Para denúncias através da Ouvidoria do Ministério Público de Minas Gerais, acesse **www.mpmg.mp.br** e clique em Serviço ao Cidadão > Ouvidoria.

Coordenadoria Estadual de Combate aos Crimes Cibernéticos – Coeciber

Rua Ouro Preto , 1.112, 2º andar - Bairro Santo Agostinho
Belo Horizonte - MG - CEP 30.170-041

(31) 3335-2452

crimedigital@mpmg.mp.br

Sites educativos

Existem vários *sites* educativos onde é possível conseguir informações úteis de como se proteger. Eis alguns deles:

www.mpmg.mp.br > Áreas de Atuação > Atuação Criminal > Portal Crimes Cibernéticos

http://antispam.br

http://cartilha.cert.br

http://www.censura.com.br

http://www.internetsegura.org

http://navegueprotegido.com.br

http://www.reclameaqui.com.br

http://www.rnp.br/cais/fraudes.php

http://www.safernet.org.br

Referências

BLOG. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation.
Disponível em: <http://pt.wikipedia.org/wiki/Blog>. Acesso em: 12 dez. 2011.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANÇA.
Disponível em: <http://www.rnp.br/cais/fraudes.php>. Acesso em: 17 jul. 2009.

COMITÊ GESTOR DA INTERNET NO BRASIL. Disponível em: <http://antispam.br>. Acesso em: 30 set. 2008.

GLOBO.COM. Saiba como se proteger de golpes no microblog Twitter. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1227406-6174,00-SAIBA+COMO+SE+PROTEGER+DE+GOLPES+NO+MICROBLOG+TWITTER.html>. Acesso em: 12 dez. 2011.

GRECO, Rogério. **Curso de Direito Penal**. 2. ed. Rio de Janeiro: Impetus, 2003. 848 p.

MINISTÉRIO PÚBLICO FEDERAL. **Manual prático de investigação de crimes cibernéticos**. São Paulo, 2006.

Navegue Protegido. Disponível em: <http://navegueprotegido.com.br>. Acesso em: 30 set. 2008.

MOVIMENTO CRIANÇA MAIS SEGURA NA INTERNET. Guia de postura em redes sociais. Disponível em: <http://www.familiamaissegura.com.br/guia-de-postura-em-redes-sociais/>. Acesso em: 8 mar. 2017.

MOVIMENTO INTERNET SEGURA. Disponível em: <http://www.internetsegura.org>. Acesso em: 2 mar. 2017.

MINISTÉRIO PÚBLICO DE MINAS GERAIS . **Diga não ao *bullying***. Belo Horizonte, 2010.
Disponível em: <https://www.mpmg.mp.br/comunicacao/producao-editorial/diga-nao-ao-bullying.htm#.WhLtZoV0HJx>. Acesso em: 9 mar. 2017.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Disponível em: <http://cartilha.cert.br>. Acesso em: 30 set. 2008.

NUTTI, Guilherme de Souza. **Manual de Processo Penal e Execução Penal**. 2. ed. revisada, atualizada e ampliada. São Paulo: Editora Revista dos Tribunais, 2006.

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**. 6. ed. 2ª tiragem. Belo Horizonte: Del Rey, 2006. 782 p.

PACHECO, Denílson Feitoza. **Direito Processual Penal. Teoria, Crítica e Práxis**. 3. ed. revisada, ampliada e atualizada com Emenda Constitucional da Reforma do Judiciário. Niterói: Impetus, 2005. 1400 p.

PRIVACIDADE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation.
Disponível em: <https://pt.wikipedia.org/wiki/Privacidade>. Acesso em: 9 mar. 2017.

RAMOS JUNIOR, Hélio Santiago. Estudo sobre a Aplicabilidade das Leis Penais aos Crimes Informáticos no Brasil. **The Third International Conference of Forensic Computer Science (ICoFCS'2008)**.
Guarujá, v. 3, n.1, p. 36-47, 2008.

RECLAME AQUI. Disponível em: <http://www.reclameaqui.com.br>. Acesso em: 16 jul. 2009.

SAFERNET BRASIL. Disponível em: <http://www.safernet.org.br/>. Acesso em: 09 mar. 2017.

WIKIPEDIA: twitter. Disponível em: <http://pt.wikipedia.org/wiki/Twitter>. Acesso em: 12 dez. 2011.

OFICINA DA NET. As dez maiores redes sociais. Disponível em: <https://www.oficinadanet.com.br/post/16064-quais-sao-as-dez-maiores-redes-sociais>. Acesso em: 2 jun. 2017.

UNIVERSIDADE FEDERAL DE SANTA MARIA. Privacidade. Disponível em: <http://www-usr.inf.ufsm.br/%7Ecacau/elc202/Privacidade.html>. Acesso em: 2 jun. 2017.

MEIO & MENSAGEM. Publicidade, um desafio para o Youtube Kids. Disponível em: <http://www.meioemensagem.com.br/home/midia/2016/07/01/lancado-no-brasil-youtube-kids-e-polemico-nos-eua.html>. Acesso em: 2 jun. 2017.

BLOG DE MARKETING DIGITAL. O que é Twitter? Para que serve? Por que faz tanto sucesso? Disponível em: <http://blogdemarketingdigital.com.br/o-que-e-twitter-pra-que-serve/>. Acesso em: 2 jun. 2017.

CUNHA, Juliana Andrade; NEJM, Rodrigo. (Org.). **Preocupado com o que acontece na Internet? Quer conversar?** 2. ed. Salvador: SaferNet, 2012. Disponível em: <www.helpline.org.br/cartilha>. Acesso em: 25 jan. 2017


MPMG
Ministério Público
do Estado de Minas Gerais