

Navegar com Segurança

Protegendo seus filhos da pedofilia
e da pornografia infantojuvenil na internet



Promotoria Estadual de Combate aos Crimes Cibernéticos

Coordenação

Mário Konichi Higuchi Júnior

Redação

Cosme Coelho Teixeira

Evandro Geraldo Ferreira Borges

Fabiana Duarte Quitite

Flaviane Lenimar Vieira Brandão Silva

Hérica Alonso Cicarelli Fonseca

Luiz Cláudio Ferreira do Nascimento

Márcia Aparecida Freitas dos Santos

Mário Konichi Higuchi Júnior

Riany Alves de Freitas

Paulo Leonardo Benício Praxedes

Vanessa Fusco Nogueira Simões

ficha técnica

Superintendência de Comunicação Integrada

Coordenação

Giselle Correia Borges

**Design gráfico,
ilustração e diagramação**

Leila Batalha

Revisão

Oliveira Marinho Ventura

Impressão

Mafali Editora

Tiragem

10.000 exemplares

sumário

1 - Orientações preventivas para o uso da internet	página 7
1.1 – Mídias sociais	página 9
(Orkut, Facebook, Hi5, Badoo, Foursquare, Twitter e outros)	
1.2 – Problemas na minha conta Facebook	página 11
1.3 – Twitter	página 16
1.4 – Mensagens instantâneas	página 19
(Comunicação mediada por computador –CMC)	
1.5 – Websites	página 22
1.6 – Blogs	página 25
1.7 – Comércio eletrônico	página 26
1.8 – Correio eletrônico (<i>e-mail</i>)	página 29
1.9 – Salas de bate-papo (<i>chats</i>)	página 33
1.10 – Softwares P2P (U-Torrent e outros)	página 36
1.11 – Jogos <i>on-line</i> (Second Life, Hotel Baboo)	página 38
1.12 – Smartphones	página 40



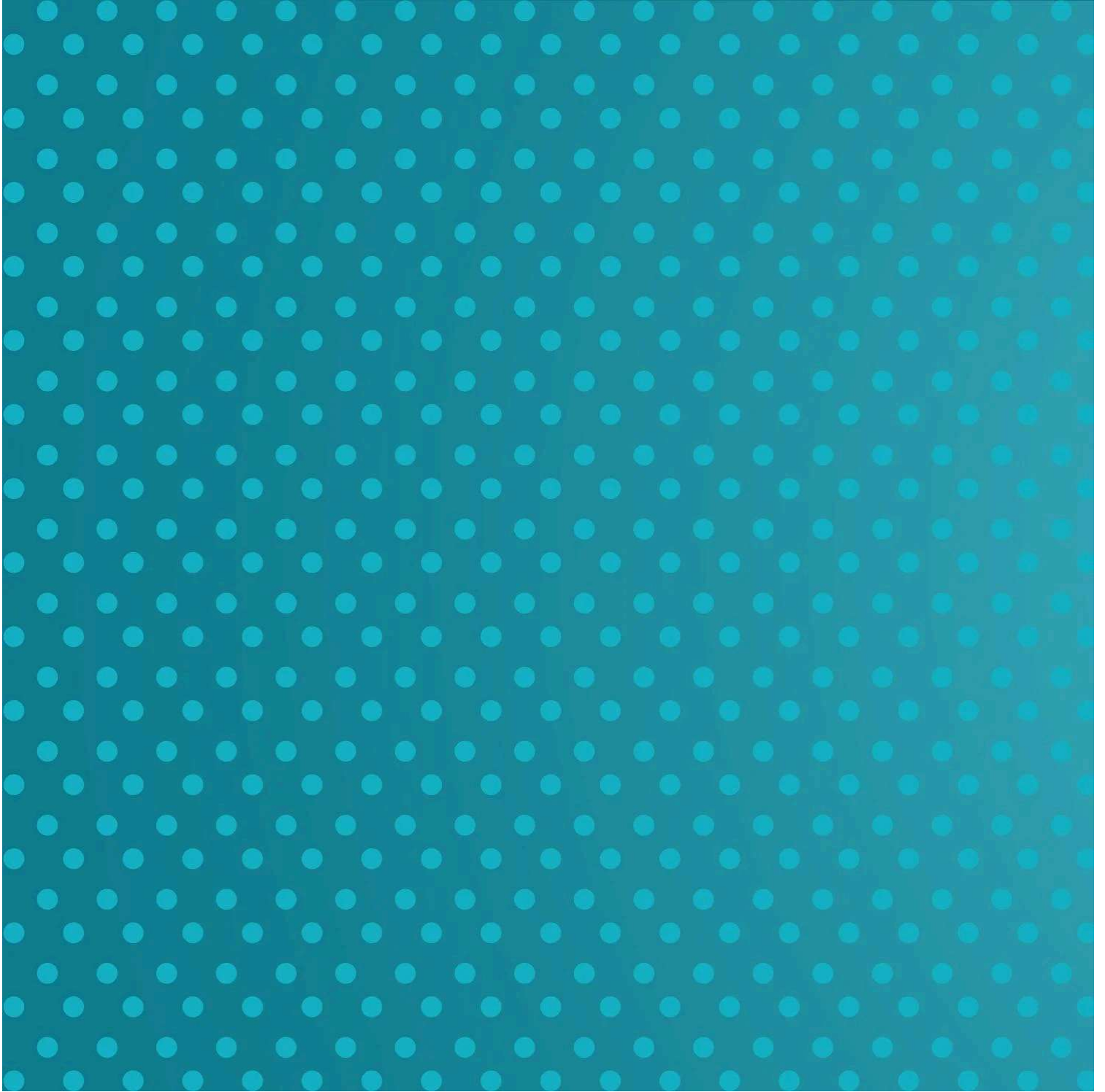
2 - Orientações para evitar acesso a conteúdo impróprio na internet	página 43
---	-----------

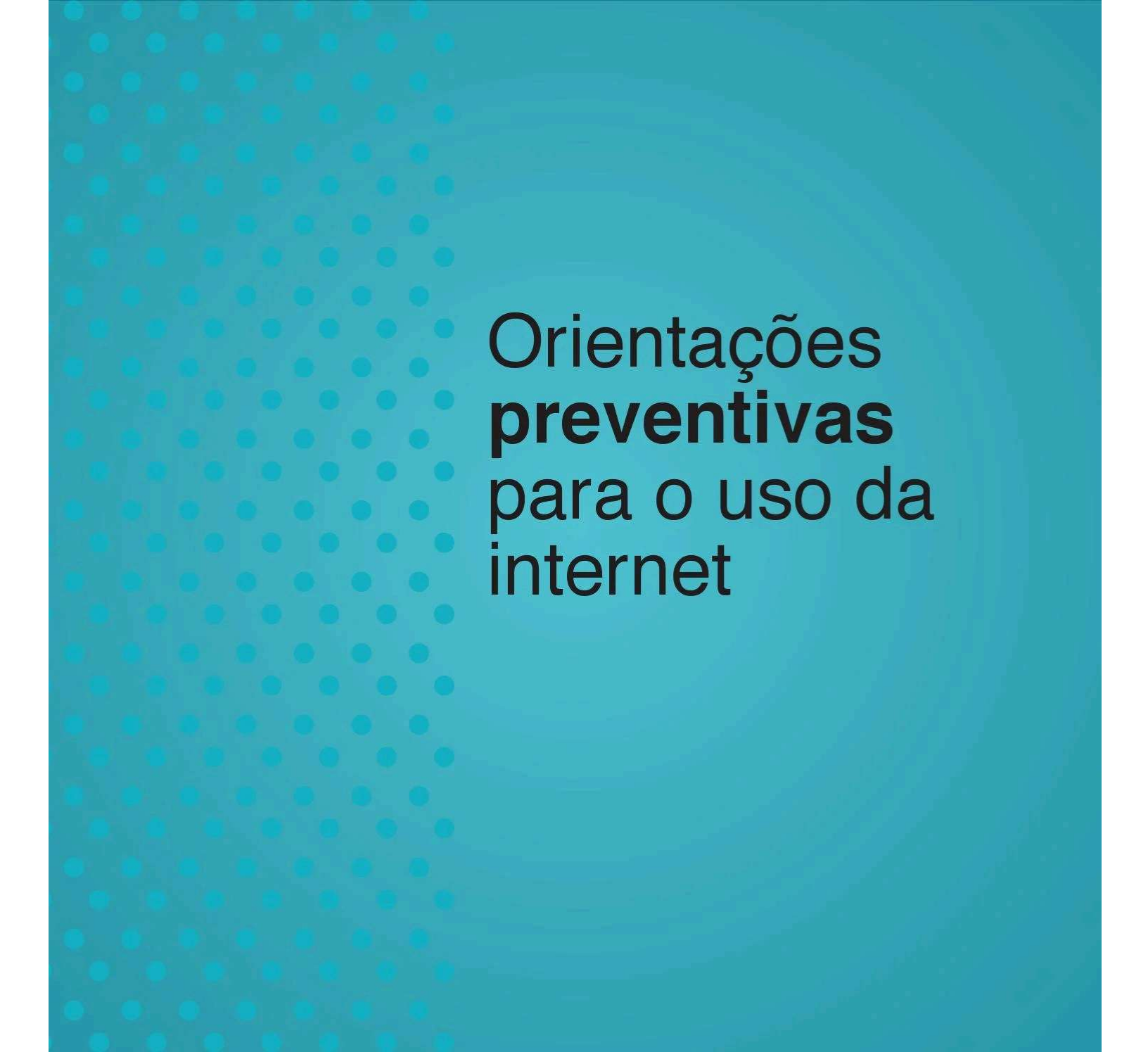
3 - Sites educativos	página 47
----------------------------	-----------

4 - Ação Penal Pública Incondicionada, Pública Condicionada e Privada	página 51
---	-----------

4.1 – Ação Penal Pública Incondicionada	página 53
4.2 – Ação Penal Pública Condicionada	página 55
4.3 – Ação Penal Privada	página 57

5 - Referências	página 59
-----------------------	-----------





Orientações **preventivas** para o uso da internet

1. **Orientações preventivas** para o uso da internet

As orientações a seguir visam a nortear uma navegação mais segura, prevenindo os internautas de se tornarem vítimas de crimes praticados na rede mundial de computadores.



1.1 - Mídias sociais

(Orkut, Facebook, Hi5, Badoo, Foursquare, Twitter e outros)

São espaços para encontro de pessoas e compartilhamento de mensagens de texto, imagens, vídeos e fotos.

Fique atento!

- Pessoas estranhas podem acessar fotos e informações pessoais inseridas nesses espaços, para fazer uso indevido delas.
- O conteúdo visualizado pode ser impróprio para menores.
- A idade mínima de acesso pode variar conforme o *site* de relacionamento; alguns indicam a idade mínima de 13 anos, outros de 14 e sucessivamente.
- No **Facebook**, a idade mínima exigida para acesso e criação de perfil é de 13 anos.
- A reputação de cada um é construída diariamente. Oriente seu filho a preservar sua boa imagem, pensando nos dias de hoje e também no futuro. Oriente-o a escolher bem as comunidades de que irá participar, evitando aquelas que podem prejudicar sua reputação.
- Eduque seus filhos a não publicar conteúdos ofensivos a outras pessoas.



Cuidados a tomar

- Oriente seu filho a utilizar as mídias sociais com inteligência, criando grupos, listas de amigos em pelo menos 3 níveis: família, amigos reais e amigos virtuais. Assim, basta compartilhar fotos com os grupos



adequados. Fotos de família devem ser compartilhadas com a família. Fotos de eventos sociais devem ser compartilhadas apenas com amigos reais. Fotos que não comprometem ou não identificam o usuário podem ser compartilhadas com os amigos virtuais.

- Não responda a provocações nem ofenda outras pessoas.
- Tenha em mente que muitos *links*, de modo geral, trazem consigo código de programa malicioso, e por isso não devem ser abertos.
- Se tiver o perfil roubado, clonado, ou sofrer difamação, imprima tudo o que possa servir como prova (conteúdo da comunidade, mensagem ou imagem ofensiva, página inicial do usuário responsável por aquele conteúdo) e procure um advogado apto a promover a ação penal e, se for o caso, requerer os dados cadastrais do ofensor.
- Na maioria dos casos, os abusos podem ser denunciados diretamente ao *site* de relacionamento.
- Oriente seus filhos, parentes e amigos a clicar em “Sair” sempre que deixar o *site* em que estiver navegando. Oriente-os a não gravar as senhas nos computadores utilizados, principalmente em *lan houses*. Se a senha for gravada, mesmo clicando em “Sair”, a conta ficará vulnerável.



1.2 - Problemas na minha conta Facebook

Conforme notícia publicada pela revista *Exame* em 17 de maio de 2012, nos últimos meses, o Brasil conquistou rapidamente o *ranking* dos países com mais usuários no Facebook, onde já ocupa o segundo lugar, atrás apenas dos Estados Unidos. Estimativas da empresa americana SocialBakers indicam que, nos últimos seis meses, 16,6 milhões de brasileiros aderiram ao Facebook, o que trouxe um aumento de 54% no total de usuários no país, agora estimados em 47 milhões.

Diante desse quadro, cresceu também o número de vítimas de delitos praticados nesse ambiente virtual.

Fique atento!

- Pessoas podem criar páginas falsas utilizando o nome de seu filho.
- Páginas falsas podem exibir conteúdo impróprio para menores, ou vender produtos falsificados ou que nunca serão entregues.
- Mídias sociais podem ser usadas para a prática de *bullying*.

Cuidados a tomar

- Se você receber um *e-mail* suspeito, fingindo ser do Facebook, encaminhe para **phish@fb.com**.



- Denuncie perfis falsos no *site*:
https://www.facebook.com/help/?faq=174210519303259&in_context



Como denunciar uma conta falsa ...

facebook Olá , em que você precisa de ajuda?

Central de ajuda » Denunciar algo Português (Brasil)

Como denunciar problemas

- Não possui uma conta?
- Denuncie uma violação
- Denunciar um erro
- Bullying
- Ferramentas para combater abusos**
- Ferramentas para pais e educadores
- Questões de autoridades e terceiros
- Problemas de propriedade intelectual >
- Direitos de privacidade de imagem
- Dê-nos sua opinião:
- Voltar

Como denunciar uma conta falsa que está fingindo ser eu?

O Facebook não permite linhas do tempo falsas criadas para imitar pessoas reais.

Se alguém criou uma conta fingindo ser você:

1. Vá até a linha do tempo
2. Clique em  e selecione **Denunciar/Bloquear**
3. Marque a caixa próxima a **Denunciar esta linha do tempo**
4. Clique em **Esta pessoa está fingindo ser alguém**
5. Selecione **Eu** no menu suspenso
6. Clique em **Continuar**
7. Adicione uma descrição do motivo por que está denunciando a linha do tempo
8. Marque a caixa próxima de **Eu confirmo que esta denúncia está correta**
9. Clique em **Continuar** para enviar sua denúncia

Report and/or Block This Person

☐ **Block Bo Jackson**
 Blocking means you won't be able to see or contact each other on Facebook

Additionally, you may file a report.

☒ **Report this profile as the following:**

- ☐ This is my old account
- ☐ This person is posting things or sending me messages I don't like
- ☒ This person is pretending to be someone

Choose a type

- ☒ **Me**
- ☐ Someone I know
- ☐ A celebrity
- ☐ A pet, cartoon or character from a game or movie

Is this your intellectual property?

Continue **Cancel**

Se alguém criou uma linha do tempo no Facebook fingindo ser você, e você não tem uma conta no Facebook, faça uma denúncia aqui.



- Denuncie páginas que possuem conteúdo impróprio, conforme orientação no site <https://www.facebook.com/help/187721894638019>

Como faço para denunciar uma p...

facebook

Central de ajuda Português (Brasil)

Comece aqui >
Gerencie sua conta >
Segurança >
Privacidade >
Feed de notícias (página inicial) >
Linha do tempo >
Compartilhamento >
Mensagens >
Conectando >
Recursos populares >
Facebook Móvel >
Aplicativos, jogos e créditos >
Gerenciando uma Página >
Anúncios e Histórias patrocinadas >
Denunciar algo >

Como faço para denunciar uma Página do Facebook?

1. Vá para a página que deseja denunciar
2. Clique no menu suspenso abaixo da capa da página
3. Selecione **Denunciar página**

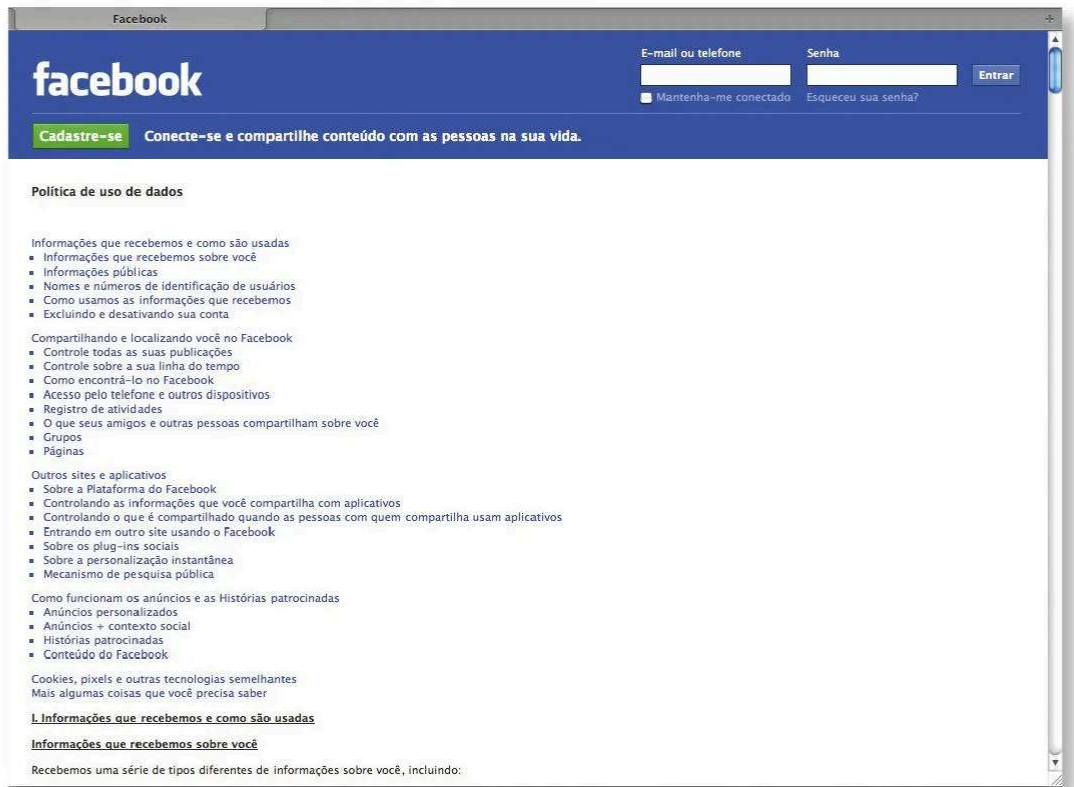


Essa resposta foi útil? [Sim](#) · [Não](#) Link permanente · Compartilhar

Facebook © 2012 · Português (Brasil) [Sobre](#) · [Criar um anúncio](#) · [Criar uma página](#) · [Desenvolvedores](#) · [Carreiras](#) · [Privacidade](#) · [Cookies](#) · [Termos](#) · [Ajuda](#)



- Acesse a página <https://www.facebook.com/legal/proposeddup/pt> sobre a Política de uso de dados e se informe sobre como os dados de seus filhos serão utilizados pelo Facebook e o que fazer para evitar a exposição indevida dessas informações.



Orientações para controlar a linha do tempo

- Sempre que você adiciona itens à sua linha do tempo, pode selecionar um público específico ou até mesmo personalizar seu público. Para fazer isso, basta clicar no ícone de compartilhamento e escolher quem pode vê-la.



- Escolha esse ícone  se desejar tornar algo **Público**. Optar por tornar algo público é exatamente o que parece. Significa que qualquer pessoa, incluindo pessoas fora do Facebook, poderá vê-las ou acessá-las.
- Escolha esse ícone  se quiser compartilhar com seus **Amigos** do Facebook.
- Escolha esse ícone  se quiser **Personalizar** seu público-alvo. Você também pode usá-lo para ocultar um item em sua linha do tempo de pessoas específicas.
- Faça o seu *check-in* sempre de forma privativa e não pública. Assim, apenas seus amigos saberão a sua localização. Os melhores *check-ins* públicos são aqueles que não irão facilitar sua localização por estranhos, por exemplo, em uma torcida durante um jogo de futebol.



- O **FourSquare** é uma mídia social como qualquer outra. Por isso, os cuidados adotados devem ser os mesmos a serem observados para as demais mídias.
- **Senha** é um segredo! Segredos são conhecidos apenas por uma pessoa. A partir do momento em que mais de uma pessoa toma conhecimento de um segredo, ele deixa de ser um segredo! Não é prova de amor compartilhar sua senha com um namorado.



- Configure a privacidade de suas fotos em ambientes como o **Instagram** ou **Flickr**. A regra básica é: apenas familiares podem ter acesso a fotos que envolvem a sua família e a sua intimidade. Amigos reais podem acessar fotos que remetem à sua privacidade e o identificam de alguma maneira. Amigos virtuais podem acessar aquelas fotos que não comprometem em nada sua segurança, como passarinhos no ninho, flores, multidões, montanhas.



1.3 - Twitter



Twitter é uma rede social e servidor para *microblogging* que permite aos usuários enviar e receber atualizações pessoais de outros contatos (em textos de até 140 caracteres, conhecidos como *tweets*), por meio do *website* do serviço, por SMS e por *softwares* específicos de gerenciamento.



Fique atento!

- Criminosos podem criar usuários falsos e robôs para envio de mensagens automatizadas.
- Um link encurtado geralmente esconde o endereço real, e pode levar o usuário a qualquer lugar, por exemplo, a um vírus ou página indesejada.
- O que você divulga no Twitter pode ser visto instantaneamente em todo o mundo.



Cuidados a tomar

- Preste atenção ao nome do usuário, verificando o perfil individual nos resultados de pesquisas. Os nomes de robôs geralmente são genéricos, simples, contendo alguns números.
- Verifique, nos *links*, a barra de endereço e a barra de status do navegador, e pare o carregamento da página se o endereço for suspeito.
- Leia Termos e Condições de Utilização dos Serviços e lembre-se: “Você é o que você Twittar!”
- Tenha cuidado com o compartilhamento de fotos no Twitter.

Delitos mais comuns praticados em mídias sociais

- **Injúria:** Art. 140 do Código Penal – “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: **Pena** - detenção, de 1 (um) a 6 (seis) meses, ou multa.”
- **Calúnia:** Art. 138 do Código Penal – “Caluniar alguém, imputando-lhe falsamente fato definido como crime: **Pena** - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.”
- **Difamação:** Art. 139 do Código Penal – “Difamar alguém, imputando-lhe fato ofensivo à sua reputação: **Pena** - detenção, de 3 (três) meses a 1 (um) ano, e multa.”

OBS.: Distinção entre injúria, calúnia e difamação: na calúnia, uma pessoa imputa falsamente a outra a prática de fato definido como crime (ex: Fulano é a pessoa que a polícia está procurando pela prática de vários roubos). Na difamação há imputação de fato ofensivo à reputação do ofendido (ex: Fulano só chega ao trabalho embriagado). Por fim, na



injúria, propala-se uma qualidade negativa da vítima, ofendendo-lhe a honra subjetiva (dignidade e o decoro) (ex: chamar alguém de ladrão, farsante, incompetente, relapso). Os crimes em questão podem ocorrer, por exemplo, com a postagem de recados em comunidades virtuais.

A ação penal, nesses casos, será privada. Significa dizer que a legitimidade para a propositura da ação penal é da vítima ou de seu representante legal. Casos como a injúria racial, todavia, são considerados crimes de ação penal pública condicionada à representação do ofendido. Nessa hipótese, o Ministério Público, titular da ação penal, só pode a ela dar início se a vítima ou seu representante legal o autorizarem, por meio de uma manifestação de vontade, no sentido de ver processado o infrator, o que pode ser feito perante o Promotor de Justiça ou na Delegacia de Polícia.

- **Incitação ao crime:** Art. 286 do Código Penal – “Incitar, publicamente, a prática de crime: **Pena** - detenção, de 3 (três) a 6 (seis) meses, ou multa.” Ocorre, por exemplo, quando alguém cria uma comunidade virtual para induzir ou estimular as pessoas a praticar uma conduta definida como crime. A ação penal, nesse caso, será pública incondicionada. Isso significa que não se impõe qualquer condição para que o Ministério Público atue. Nesse caso, os crimes afetam sobremaneira o interesse geral, razão pela qual a necessidade que tem o Estado de ver reprimido o crime é maior do que a do ofendido.
- **Racismo:** Art. 20 da Lei n.º 7.716/89, com redação dada pela Lei n.º 9.459/97 - “Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. **Pena:** reclusão de um a três anos e multa”. A ação penal, nesse caso, será pública incondicionada. Casos de racismo deverão ser comunicados ao Ministério Público Federal.



1.4 - Mensagens instantâneas (Comunicação mediada por computador –CMC)

Permitem conversar pela internet, em tempo real, com o interlocutor que estiver conectado.

Fique atento!

- Pessoas estranhas podem simular-se conhecidas e obter informações pessoais ou imagens nas conversas.
- Todo o conteúdo transmitido por meio desse recurso pode ser divulgado em diversos países.
- Mensagens de conteúdo ofensivo podem ser trocadas nesse ambiente.
- Pode haver disseminação de código malicioso.



*Exemplo de tentativa
de inserção de código
malicioso (vírus)*





*Exemplo de tentativa
de inserção de código
malicioso (vírus)*

Cuidados a tomar

- Não poste fotos ou informações pessoais na internet.
- Não mostre imagens suas, ou do ambiente em que se encontra, a estranhos. Cuidado ao exibir-se na webcam! Nunca se sabe para onde essas imagens serão enviadas. Às vezes, são publicadas no exterior, o que dificulta a remoção desse conteúdo.
- Tenha em mente que muitos links, de modo geral, trazem consigo código de programa malicioso, e por isso não devem ser abertos.
- Grave sempre as conversas em ambientes de CMC.
- Se tiver conhecimento de infração cometida por meio de mensagens instantâneas, providencie a impressão das conversas salvas, além das



informações sobre o interlocutor (números identificadores, apelidos ou e-mail), anotando a data e o horário da comunicação. Com todas essas informações, procure um advogado, em se tratando de crime de ação penal privada, ou uma Delegacia especializada ou o Ministério Público, no caso de crimes que se processam mediante ação penal pública.

- Oriente seus filhos, parentes e amigos a observar essas recomendações.

Delitos mais comuns praticados por meio de mensagens instantâneas

- Pornografia Infantil: Art. 241-A do Estatuto da Criança e do Adolescente - “Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: **Pena** – reclusão, de 3 (três) a 6 (seis) anos, e multa”. Dá-se, por exemplo, quando alguém envia fotos de crianças ou adolescentes em cena de sexo explícito.
- Art. 241-D do Estatuto da Criança e do Adolescente - “Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: **Pena** – reclusão, de 1 (um) a 3 (três) anos, e multa”.
- Art. 244-B do Estatuto da Criança e do Adolescente - “Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la: **Pena** - reclusão, de 1 (um) a 4 (quatro) anos. § 1º Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet”.

A ação penal, nestes casos, será pública incondicionada.



1.5 - Websites

São páginas da internet nas quais o internauta pode navegar, fazer pesquisas, compras, entre muitas outras funcionalidades.

Fique atento!

- As páginas podem ser falsas.
- Domínios cadastrados no estrangeiro dificultam a ação da polícia; por exemplo, endereços de final “.com”.

Cuidados a tomar

- Atente a páginas que apresentam conteúdo pornográfico e impróprio para crianças.
- Faça o *download* de programas diretamente do *site* do fabricante.
- Se tiver conhecimento de infração cometida num *site* da internet, imprima as páginas e procure um advogado, caso se trate de infração cuja ação penal seja privada. Procure a Delegacia especializada ou o Ministério Público em caso de crimes de ação penal pública, ou na hipótese de impossibilidade de obtenção imediata de provas bastantes para a propositura da ação penal privada.



- Capture as páginas criminosas para apresentá-las à autoridade responsável pelas investigações. Isso pode ser feito através da tecla <PrintScreen>. Nas capturas, é importante confirmar se aparece o endereço da página (ou url), conforme o exemplo a seguir:



Delitos mais comuns praticados em páginas da internet

- **Favorecimento à prostituição:** Art. 228 do Código Penal – “Induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone: **Pena** - reclusão, de 2 (dois) a 5 (cinco) anos”. Ocorre, por exemplo, quando alguém publica página na internet para intermediar ou facilitar a prática da prostituição.
- **Rufianismo:** Art. 230 do Código Penal – “Tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça: **Pena** - reclusão, de 1 (um) a 4 (quatro) anos, e multa”. Ocorre quando alguém publica página na internet, oferecendo pessoas à prática da prostituição, e tira proveito econômico disso.
- **Violação de direito autoral:** Art. 184 do Código Penal – “Violar direitos de autor e os que lhe são conexos: **Pena** - detenção, de 3 (três) meses a 1 (um) ano, ou multa”. Dá-se, por exemplo, quando alguém publica obra intelectual na internet sem citar o nome do autor e sem possuir expressa autorização para sua reprodução ou para modificar o conteúdo da obra intelectual.

A ação penal, em qualquer dos casos acima, será pública incondicionada.

- **Violação de direito de autor de programa de computador:** Art. 12 da Lei n.º 9.609/98 – “Violar direitos de autor de programa de computador: **Pena** - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: **Pena** - Reclusão de um a quatro anos e multa.”

A ação penal, nessas hipóteses, é privada.



1.6 - Blogs

Um blog é um *site* cuja estrutura permite a atualização rápida a partir de acréscimos de artigos, ou *posts*, organizados, em geral, de forma cronológica inversa, tendo como foco a temática proposta do blog, podendo ser escritos por um número variável de pessoas, de acordo com a política do blog.

Fique atento!

- O anonimato é proibido no Brasil. Por isso, todo conteúdo deve conter a identificação do responsável.
- Os conteúdos publicados podem ser falsos e ofensivos.

Cuidados a tomar

- Mostre-se educado, ético e responsável. Evite publicar conteúdos ofensivos e difamatórios, que ridicularizem outras pessoas.
- Verifique a veracidade das informações antes de publicá-las.
- Somente utilize imagens de outras pessoas se for previamente autorizado por elas.
- Não publique informações pessoais ou relacionadas à sua rotina diária, ou à de sua família.
- Respeite os direitos autorais na internet, citando a fonte de referência do conteúdo utilizado.
- Oriente seu filho a não publicar conteúdos falsos e ofensivos e a não se expor na internet, chamando-lhe a atenção para todos esses cuidados.



1.7 - Comércio eletrônico

São espaços para a compra de produtos e serviços pela internet.

Fique atento!

- Pessoas mal-intencionadas criam *sites* falsos para vender produtos que nunca serão entregues.
- Domínios cadastrados no estrangeiro dificultam a ação da polícia. Por exemplo, endereços de final “.com”.
- Em *sites* de leilões, é comum haver uma espécie de robô, que acompanha os leilões e efetua o lance automaticamente para sempre ganhar e lesar os usuários.

Cuidados a tomar

- Não efetue compras em *sites* sem boa procedência. Verifique com pessoas conhecidas se já compraram no *site* escolhido e receberam o produto. Consulte se há reclamações sobre o vendedor no endereço **www.reclameaqui.com.br**.
- Antes da compra, realize uma busca sobre o vendedor nos *sites* de busca, como Google, Bing, Yahoo. Assim, você perceberá se há reclamações de outros usuários.
- Crie uma conta de *e-mail* específica para compras na internet.



- Desconfie de propostas muito boas, produtos milagrosos ou de preço muito inferior ao de mercado.
- Dê preferência a pagamentos via boleto bancário. De posse do boleto, o usuário poderá realizar o pagamento pela internet por meio do código de barras. Antes de finalizar o pagamento, o usuário deverá atentar para o nome do recebedor. Pessoas físicas ou contas poupança são sempre um bom motivo para desconfiar da idoneidade de *sites*. É que os confiáveis normalmente recebem pagamentos em nome da empresa e não de pessoas físicas.
- Consulte o *site* de vendas no **www.registro.br** e verifique os dados completos de quem registrou o domínio, o CNPJ e o endereço da empresa responsável.
- Ofereça o mínimo possível de informações para completar a transação. Evite acrescentar dados que não tenham relação alguma com a concretização do negócio.
- Procure certificar-se de que todas as informações fornecidas pelo *site* estão corretas, como razão social, CNPJ, endereço e telefone de contato. Tenha cuidado quando o *site* fornecer como forma de contato apenas telefone celular ou conta de comunicador instantâneo (CMC).
- Não forneça senhas a ninguém. Proteja suas informações pessoais com senhas fortes, escolhendo uma sequência aleatória entre 8 e 12 caracteres, alternando letras minúsculas, letras maiúsculas, números e símbolos. Evite sequências ou caracteres repetidos. Troque sua senha regularmente.
- Verifique a política de privacidade da loja virtual. Saiba qual o compromisso do vendedor em relação à manipulação dos dados que você informa.



- Evite também 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.
- Confirme na página do fabricante do produto se as características deste condizem com as fornecidas pelo *site* do vendedor.
- Verifique as características do produto, condições de entrega, tarifas de envio, formas de pagamento e condições de troca.
- Registre toda a negociação e transação, como *e-mails*, anúncios, as telas do *site* de compra e toda a comunicação estabelecida com a loja. Caso seja vítima de estelionato, registre sua denúncia, com todos os comprovantes, na página da Promotoria Estadual de Combate aos Crimes Cibernéticos. Informe o endereço do *site*, as contas bancárias envolvidas na transação, as mensagens enviadas e recebidas, e qualquer outra informação que conseguir. Isso facilitará a investigação.

Delito mais comum praticado por meio de comércio eletrônico

- **Estelionato:** Art. 171 do Código Penal – “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. **Pena** - reclusão, de 1 (um) a 5 (cinco) anos, e multa”. Dá-se principalmente pelo envio de mensagens fraudulentas ou clonagem de páginas visando a induzir a pessoa em erro para obter vantagem econômica indevida, como pessoas mal-intencionadas anunciando produtos e serviços que nunca serão entregues; *sites* falsos criados com o propósito de fazer o internauta comprar algo, ou até mesmo se cadastrar na intenção de ganhar lucros trabalhando em casa, todavia sem que isso de fato aconteça.



1.8 - Correio eletrônico (*e-mail*)

Fique atento!

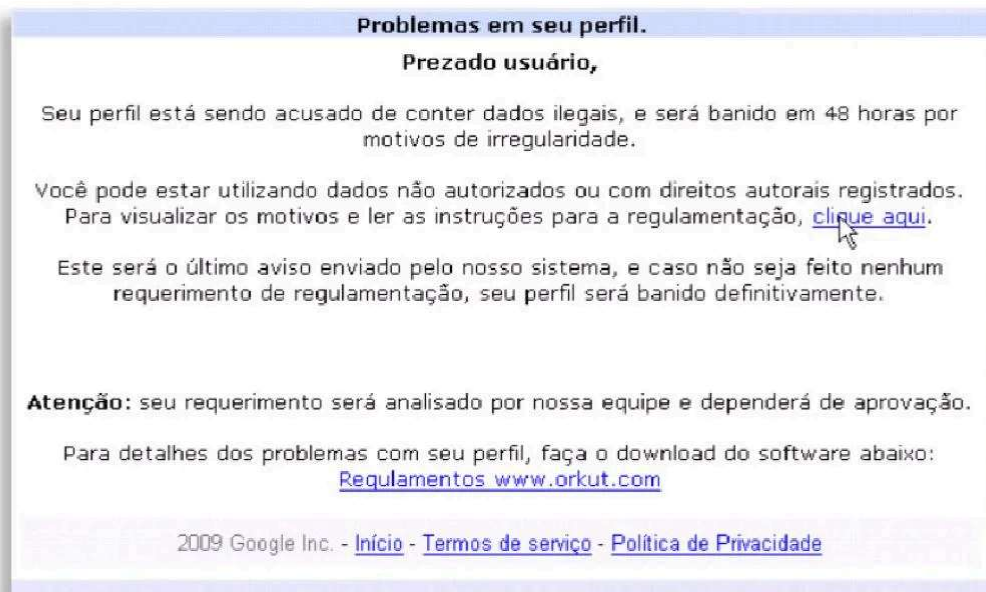
- Os *e-mails* podem trazer *links* e anexos que danificam o computador ou enviam informações (como senhas) a pessoas desconhecidas e mal-intencionadas na rede.
- As mensagens recebidas podem conter informações falsas.
- Instituições governamentais geralmente não enviam *e-mails* solicitando informações dos cidadãos.
- Crianças podem receber conteúdos impróprios.

Cuidados a tomar

- Não abra *e-mails* de pessoas desconhecidas.
- Tenha sempre um antivírus atualizado! Prefira as versões pagas, pois são confiáveis e possuem ferramentas abrangentes de proteção e bloqueio.
- Não abra anexos de *e-mails* que considere irrelevantes ou cuja procedência desconheça.
- Oriente o seu filho a observar essas recomendações.
- Crie uma conta de *e-mail* própria para assuntos pessoais, uma para assuntos profissionais e outra para compras na internet.
- Não acredite em *e-mails* que o induza a clicar num *link* ou preencher informações pessoais.



- Verifique as fraudes registradas, comumente recebidas por *e-mail*, na página eletrônica do Centro de Atendimento a Incidentes de Segurança (CAIS): <http://www.rnp.br/cais/fraudes.php>.
- Se tomar conhecimento de uma infração, salve-a e imprima o *e-mail*, verificando se a opção 'Exibir/Cabeçalhos' está ativa, pois o cabeçalho será importante para as investigações. Depois, procure um advogado, em se tratando de crime de ação penal privada, ou uma Delegacia especializada ou o Ministério Público, no caso de crimes que se processam mediante ação penal pública.
- Feche o programa de *e-mail* utilizando a opção 'Sair'.



Exemplo de tentativa de *phishing*, ou seja, de “pescar” dados do internauta. Trata-se de *e-mail* falso. Não clique nos *links* de *e-mails* como esse, pois objetivam capturar suas informações pessoais para uso indevido.



Delitos mais comuns praticados mediante *e-mails*

- **Ameaça:** Art. 147 do Código Penal – “Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: **Pena** - detenção, de 1 (um) a 6 (seis) meses, ou multa”. Pode ocorrer, por exemplo, por meio do envio de mensagens eletrônicas ou recados virtuais com o intuito de intimidar a vítima, ameaçando-a de causar mal injusto ou grave. A ação penal, nesse caso, será pública condicionada à representação.
- **Dano:** Art. 163 do Código Penal – “Destruir, inutilizar ou deteriorar coisa alheia: **Pena** - detenção, de 1 (um) a 6 (seis) meses, ou multa”. Quando alguém, por exemplo, envia vírus de computador por *e-mail* com o intuito de inutilizar o computador do destinatário. A ação penal, nesse caso, será privada, assim como na hipótese em que o dano for cometido por motivo egoístico, ou causar prejuízo considerável à vítima (art. 163, parágrafo único, inciso IV, combinado com o art. 164, ambos do Código Penal).
- **Extorsão:** Art. 158 do Código Penal – “Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar fazer alguma coisa: **Pena** - reclusão, de 4 (quatro) a 10 (dez) anos, e multa.” Bom exemplo é o da pessoa que envia mensagens eletrônicas para constranger alguém, utilizando-se de grave ameaça, com o intuito de obter vantagem econômica indevida. A ação penal, nesse caso, será pública incondicionada.



- **Invasão de dispositivo informático:** Art. 154-A do Código Penal (acrescido pela Lei 12.737/2012) – “Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: **Pena** - detenção, de 3 (três) meses a 1 (um) ano, e multa”.

§3º do art. 154-A - “Se da invasão resultar a obtenção de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: **Pena:** reclusão de 6 meses a 2 anos, e multa, se a conduta não constitui crime mais grave.” A ação penal, nesse caso, será pública condicionada à representação. Obs.: O acréscimo do artigo 154-A ao Código Penal entrará em vigor em 03/04/2013.



1.9 - Salas de bate-papo (*chats*)

São espaços para conversar com diversas pessoas ao mesmo tempo.

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.
- Pessoas mal-intencionadas buscam obter informações pessoais para uso indevido.
- O conteúdo das conversas pode ser impróprio para menores.
- Normalmente são trocadas 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.
- Não acredite em nicknames (apelidos) (ex: Advogada, Lindo e charmoso). Eles são utilizados por pessoas mal-intencionadas para iludir e ganhar a confiança de usuários.





Exemplo de apelidos postados
em sala de bate-papo

Cuidados a tomar

- Não permita que seu filho acesse as salas de bate-papo sem o acompanhamento devido.
- Não poste fotos ou informações pessoais na internet e oriente o seu filho a não o fazer.
- Os *links* geralmente trazem consigo código de programa malicioso e, por isso, não devem ser abertos.
- Se tomar conhecimento de delito praticado em sala de bate-papo, imprima o conteúdo da conversa, anote o endereço do *site* onde o serviço funciona, o nome da sala, os apelidos utilizados na conversa, a sua data e hora. De posse dessas informações, procure um advogado caso tenha informações e provas suficientes para a propositura da ação se esta for de natureza privada. Procure a Delegacia especializada se não houver informações e provas bastantes para a propositura da ação, ou o Ministério Público, em se tratando de infração cuja ação penal seja pública.



Delitos mais comuns praticados em salas de bate-papo

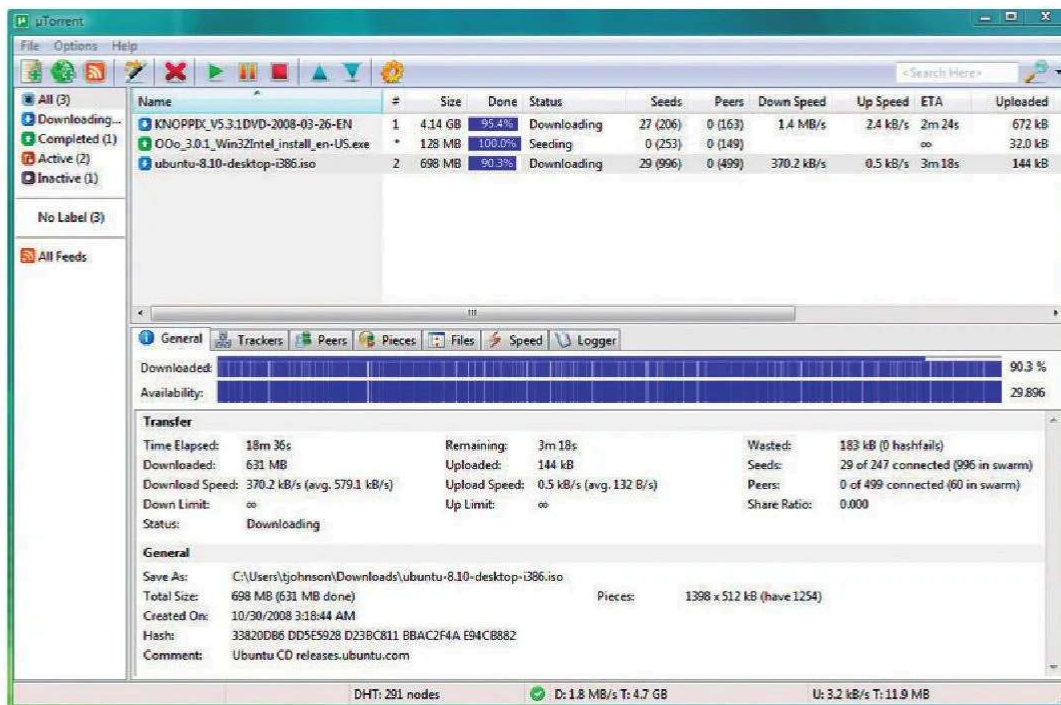
- **Pornografia Infantil:** Art. 241-A do Estatuto da Criança e do Adolescente - “Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: **Pena** – reclusão, de 3 (três) a 6 (seis) anos, e multa”. Dá-se quando alguém envia fotos de crianças ou adolescentes em cena de sexo explícito.
- Art. 241-D do Estatuto da Criança e do Adolescente - “Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: **Pena** – reclusão, de 1 (um) a 3 (três) anos, e multa”.
- Art. 244-B do Estatuto da Criança e do Adolescente: “Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la: **Pena** - reclusão, de 1 (um) a 4 (quatro) anos. § 1º Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet”.

A ação penal, nesses casos, será pública incondicionada.



1.10 - Softwares P2P (U-Torrent e outros)

São espaços que permitem o compartilhamento de arquivos armazenados em estações espalhadas por todo o mundo. A autenticação de usuários é feita, normalmente, por servidores localizados em países que não adotam legislação rígida em relação à internet, o que dificulta a identificação de um criminoso.



Fique atento!

- A prática de troca de conteúdo sem aquisição de licenças constitui delito de violação de direitos autorais.
- É comum encontrar nesse ambiente todo e qualquer tipo de arquivo, até mesmo pornografia infantil.
- Muitos vírus são disseminados por esse tipo de estrutura.

Cuidados a tomar

- Instale filtros de conteúdo e mantenha o seu computador protegido. Procure um profissional de informática para auxiliá-lo.

Delitos mais comuns praticados por meio de redes P2P

- **Pornografia Infantil:** Art. 241-A do Estatuto da Criança e do Adolescente - “Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: **Pena** – reclusão, de 3 (três) a 6 (seis) anos, e multa”. Ocorre, por exemplo, quando alguém envia fotos de crianças ou adolescentes em cena de sexo explícito.
- **Violação de direito autoral:** Art. 184 do Código Penal – “Violar direitos de autor e os que lhe são conexos: **Pena** - detenção, de 3 (três) meses a 1 (um) ano, ou multa.” Dá-se, por exemplo, por meio do compartilhamento de músicas, vídeos, imagens ou obras intelectuais sem citar o nome do autor e sem possuir expressa autorização para sua reprodução.

Nos casos acima mencionados, a ação penal será pública incondicionada.



1.11 - Jogos *on-line* (Second Life, Hotel Baboo)

São chamados *on-line* os jogos eletrônicos disputados via internet. Neles, um jogador com um computador ou video game conectado à rede pode jogar com outros sem que ambos precisem estar no mesmo ambiente. Sem sair de casa, o jogador pode desafiar adversários que estejam em outros lugares do país, ou até do mundo.



Exemplo de tela do jogo Second Life

Fique atento!

- Tem sido comum o usuário adquirir créditos no *site* do jogo e em seguida ser banido por algum motivo, geralmente descrito no contrato.
- Podem ocorrer tentativas de subtração de dados pessoais na plataforma de jogos *on-line*. Isso se deve a brechas de segurança que permitem o envio mensagens aos usuários do jogo, com o objetivo de conseguir acesso a informações privadas.

Cuidados a tomar

- Instale um antivírus na versão comercial.
- Crie uma conta no jogo e conheça o ambiente que seus filhos estão frequentando.
- Não efetue compras em *sites* sem boa procedência. Verifique com pessoas conhecidas se já compraram créditos no *site* escolhido e receberam os utilizaram sem problemas. Consulte se há reclamações sobre o jogo no endereço **www.reclameaqui.com.br**.
- Crie uma conta de *e-mail* específica para o jogo, se necessário.
- Verifique a política de privacidade do *site*. Saiba qual o compromisso do provedor do serviço em relação à manipulação dos dados que você informa.
- Mantenha os jogos sempre atualizados. Aplique sempre as correções de falhas disponibilizadas pelo fornecedor do jogo.



1.12 - Smartphones

Smartphones podem facilitar o acesso a informações disponíveis na *web*. Estudantes que usam bem os seus *smartphones* ou celulares com acesso à internet têm sempre à mão um instrumento importante para reduzir o esforço e aumentar o aproveitamento dos seus cursos.



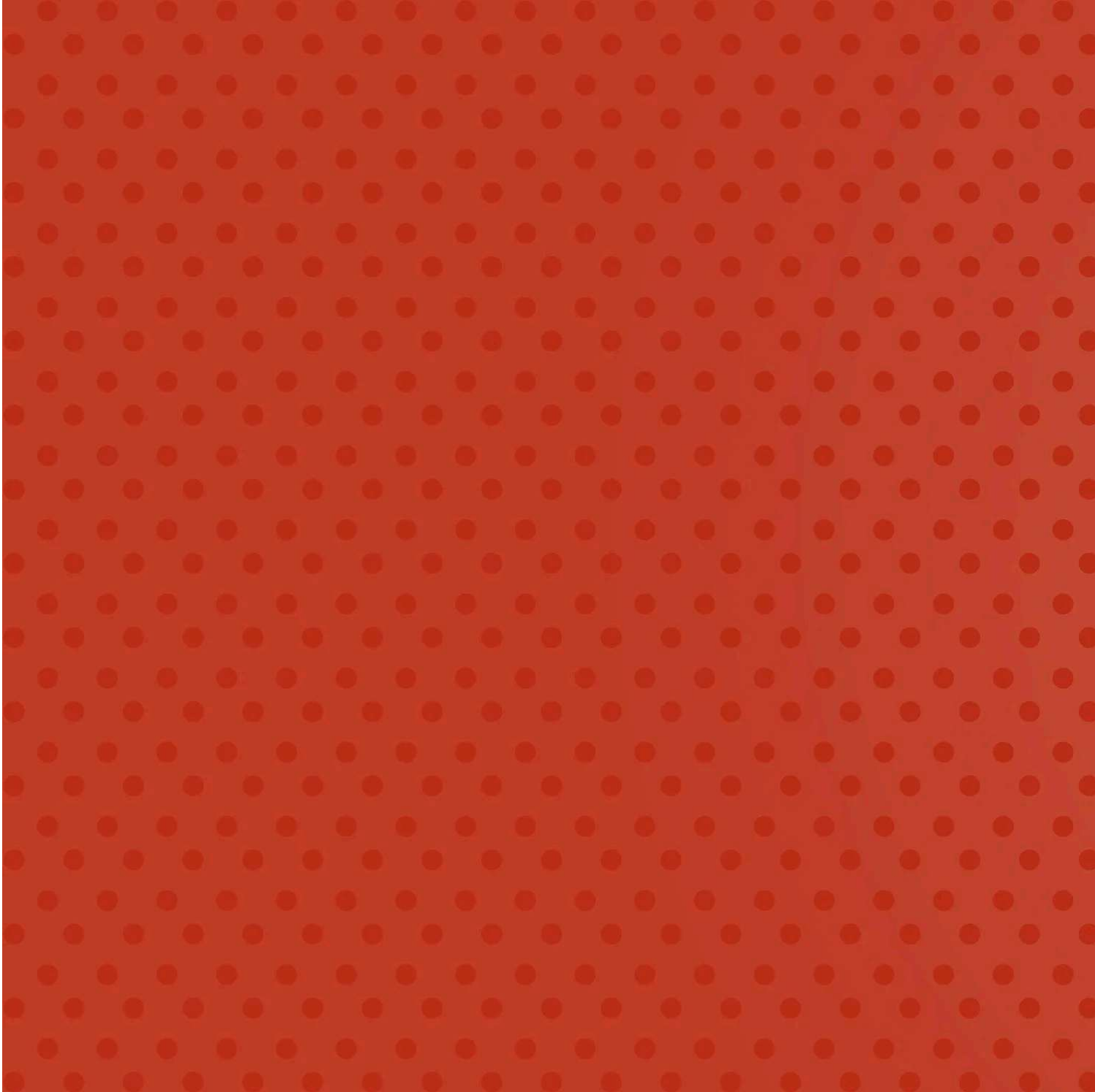
Fique atento!

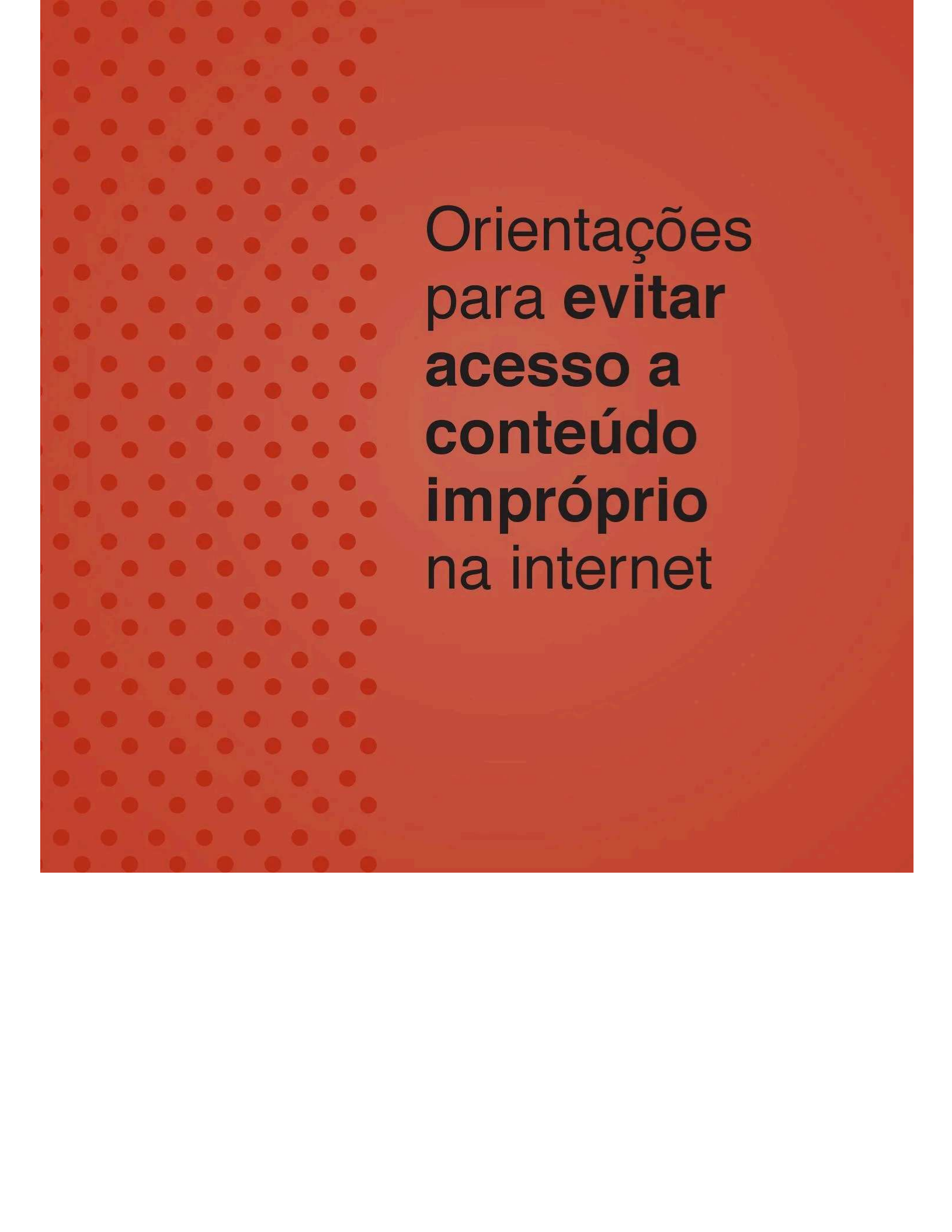
- É importante conhecer as regras da escola a respeito do uso de tecnologias móveis no ambiente escolar antes de permitir que seu filho utilize esse recurso em sala de aula. Talvez seja necessária uma autorização da coordenação para fazê-lo.
- *Smartphones* podem conter conta de *e-mail*, senhas, fotos, arquivos, e a chance de perdê-los é bem maior.

Cuidados a tomar

- Proteja o *smartphone* com senha. Oriente seus filhos a ter cuidado com as informações nele guardadas.
- Instale aplicativos de localização do equipamento para encontrá-lo em caso de perda, furto ou roubo.
- Oriente seus filhos para que não tirem fotos sensuais nem se exponham publicamente, pois podem ser fotografados, filmados e ter suas imagens disseminadas sem sua autorização.
- Desative as redes que não estão sendo utilizadas, como *wi-fi* e *bluetooth*.







Orientações
para **evitar**
acesso a
conteúdo
impróprio
na internet

2. Orientações para evitar acesso a conteúdo impróprio na internet

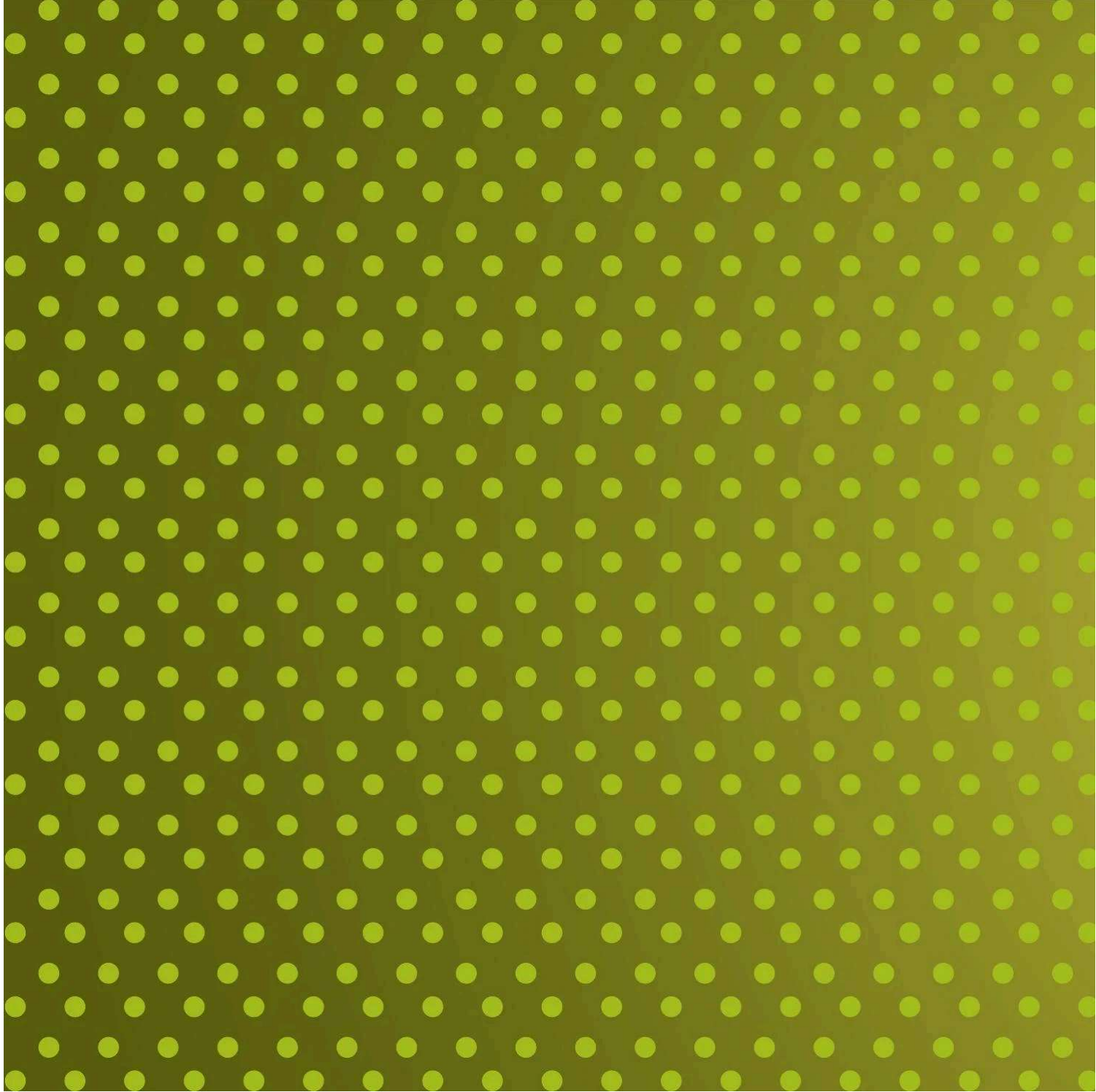
Orientamos os internautas a solicitar ajuda a um profissional de informática a fim de que ele proceda às configurações necessárias com vistas a manter o computador sempre protegido. Além disso, peça-lhe que ensine a utilizar filtros de segurança, assim como filtros de páginas e registro de todas as atividades executadas no ambiente da internet. Desse modo, ser-lhe-á possível ficar alerta e controlar as tarefas que o seu filho pode executar. A seguir, apresentamos algumas orientações para evitar que a criança tenha acesso a conteúdo impróprio na internet.

- Navegue com o seu filho alguns minutos por dia. Conheça o ambiente que ele utiliza para se divertir.
- Aconselhe seu filho a não transmitir informações pessoais, como nome, endereço, escola em que estuda, e a não distribuir fotos pela internet. Ensine-o a ser discreto nesse ambiente, principalmente com pessoas que acabou de conhecer.
- Oriente seu filho a não receber nem executar arquivos de pessoas desconhecidas.



- Conheça as pessoas com as quais seu filho se relaciona.
- Não permita que seu filho marque encontros com pessoas que conheceu na internet. Se julgar necessário, faça-os em local público, acompanhando-o sempre.
- Evite acomodar o computador no quarto ou em lugares isolados da casa. Dê preferência a lugares em que haja ampla circulação de pessoas.
- Não abra a sua *webcam* para desconhecidos: ela pode colocar um criminoso dentro da sua casa.
- Verifique sempre a idade mínima indicada para cada jogo.
- Estabeleça regras e limites para o uso da internet, de acordo com a idade de seu filho. Estipule um tempo limite ao acesso. Informe a ele os *sites* e serviços que pode ou não acessar e explique-lhe o motivo.
- Monitore o uso e as conversas. Procure informar-se sobre os recursos de segurança de seu provedor de acesso. Faça o bloqueio de todos os *sites* ou conteúdos que considere inapropriados ao seu filho. Utilize também programas de filtros de conteúdo.
- Eduque seu filho a navegar na internet com responsabilidade. Explique-lhe como proceder caso encontre um material inapropriado.
- Mantenha-se sempre próximo a seu filho. A orientação e a conversa são a melhor forma de se precaver contra os transtornos ocasionados pelo mau uso da internet.
- Instale um controlador de conteúdo. Por exemplo, o Controle dos Pais da Microsoft. Basta baixar e instalar o Windows Live Essentials no *link* <http://go.microsoft.com/fwlink/?LinkID=255475> ou buscar pelo aplicativo na página da Microsoft.



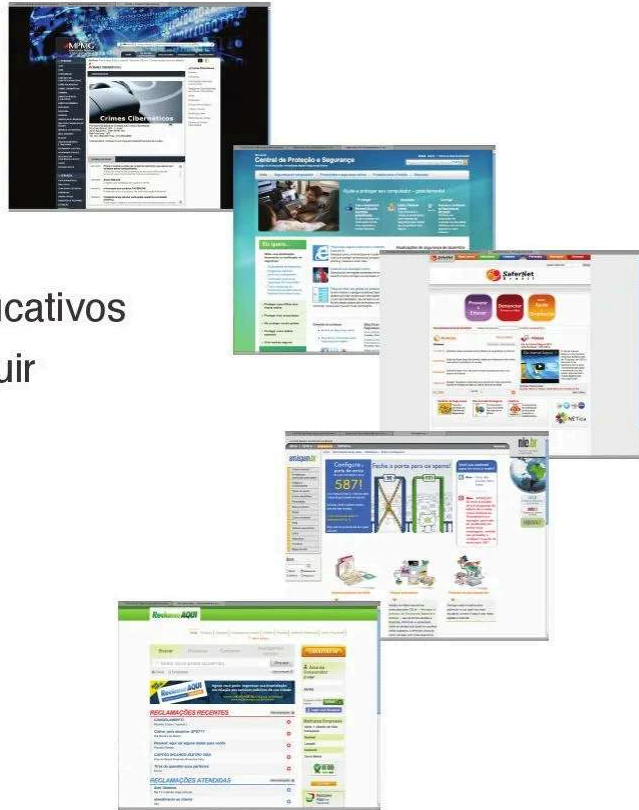




Sites educativos

3. Sites educativos

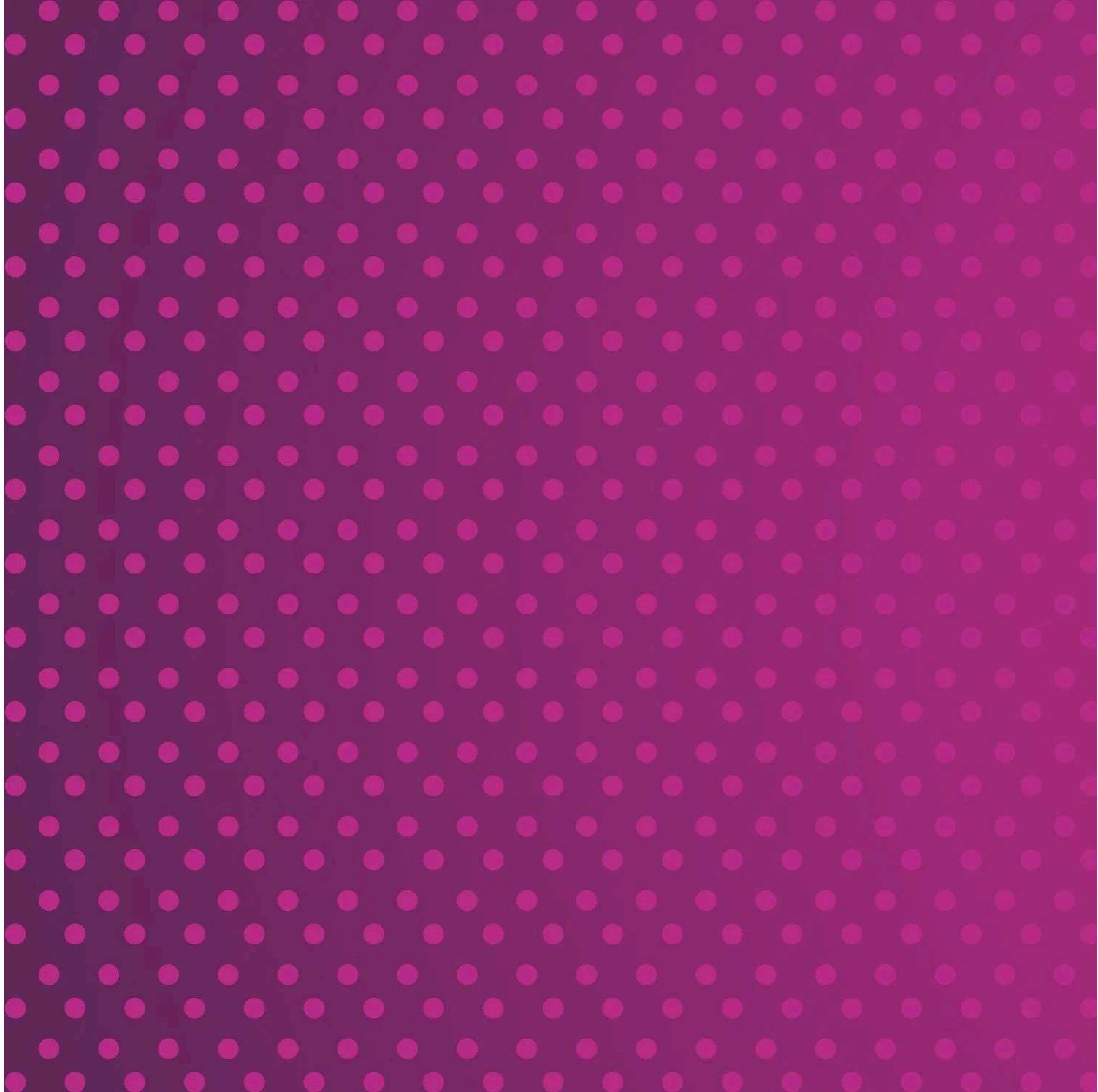
Existem vários sites educativos onde é possível conseguir informações úteis de como se proteger.



Eis alguns deles:

- <http://antispam.br>
- <http://cartilha.cert.br>
- <http://www.censura.com.br>
- <http://www.internetsegura.org>
- www.mp.mg.gov.br/ - Portal Crimes Cibernéticos
- <http://navegueprotegido.com.br>
- <http://www.reclameaqui.com.br>
- <http://www.rnp.br/cais/fraudes.php>
- <http://www.safernet.org.br>
- <http://pcworld.uol.com.br/dicas/2008/10/09/proteja-seus-filhos-monitorando-e-limitando-o-que-eles-fazem-no-pc>







Ação Penal

Pública

Incondicionada,

Pública

Condicionada

e Privada

4. Ação Penal

Pública Incondicionada,
Pública Condicionada e
Privada

Quando falamos em ação, estamos nos referindo ao direito de se pedir ao Estado a tutela jurisdicional. Assim, ação penal é o direito de se pedir ao Juiz a aplicação do direito penal a um caso concreto.

No Processo Penal, é comum a classificação das ações de acordo com a qualidade de seu titular, daí falarmos em ação penal pública (cujo titular é o Ministério Público) e ação penal privada (cujo titular é a vítima ou seu representante legal).



4.1 - Ação penal pública incondicionada

Dizemos que a ação penal é pública incondicionada quando não se impõe qualquer condição para que o Ministério Público atue. De acordo com o art. 27 do Código de Processo Penal, qualquer pessoa poderá provocar a iniciativa do Ministério Público, nos casos em que caiba a ação pública, fornecendo-lhe, por escrito, informações sobre o fato, indicando o tempo, o lugar e os elementos de convicção acerca do delito.

De posse dessas informações, basta comunicar a notícia-crime no sistema da Promotoria Estadual de Combate aos Crimes Cibernéticos, no endereço **<http://www.mp.mg.gov.br>** (Clicar em Crimes Cibernéticos), mencionando o *e-mail* para contato.

Caso possua algum documento que possa servir como prova, deve enviá-lo ao *e-mail* **crimedigital@mp.mg.gov.br**, com a informação do número da denúncia fornecido pelo sistema de denúncias da Promotoria Estadual de Combate aos Crimes Cibernéticos, ou efetuar um complemento da denúncia no sistema da Promotoria, anexando os arquivos.



Abaixo estão alguns exemplos de infrações penais cuja ação penal é pública incondicionada:

- **Apologia/incitação ao crime** (arts. 286 e 287 do Código Penal);
- **Constrangimento ilegal** (art. 146 do Código Penal);
- **Estelionato** (art. 171 do Código Penal);
- **Extorsão** (art. 158 do Código Penal);
- **Induzimento, instigação ou auxílio a suicídio** (art. 122 do Código Penal);
- **Favorecimento à prostituição** (art. 228 do Código Penal);
- **Pedofilia** (art. 241 do Estatuto da Criança e do Adolescente);
- **Racismo** (art. 20 da Lei n.º 7.716/89, com a redação dada pela Lei n.º 9.459/97);
- **Rufianismo** (tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça) (art. 230 do Código Penal);
- **Tráfico de entorpecentes** (art. 33 da Lei 11.343/06);
- **Tráfico de pessoas** (art. 231 do Código Penal);



4.2 - Ação penal pública condicionada à representação

- **Violação de direito autoral** (art. 184 do Código Penal).

Nessa hipótese, o Ministério Público, titular da ação penal, só pode a ela dar início se a vítima ou seu representante legal o autorizarem, por meio de uma manifestação de vontade, no sentido de ver processado o infrator. Ressalte-se que não são necessárias formalidades na representação. Assim, basta a declaração de vontade do ofendido ou de seu representante legal para possibilitar ao Ministério Público apurar os fatos narrados, a fim de formar a sua convicção para, se for o caso, dar início à ação penal.

É importante, se possível, a apresentação das seguintes informações: narração do fato, com todas as circunstâncias; a individualização do suposto autor do fato ou seus sinais característicos; as razões de convicção ou de presunção de ser ele o autor da infração e, ainda, a apresentação das provas conseguidas, o que facilitará a investigação.

De posse dessas informações, basta comunicar a notícia-crime na página da Promotoria Estadual de Combate aos Crimes Cibernéticos (www.mp.mg.gov.br - Clicar em Crimes Cibernéticos), mencionando nome, CPF e *e-mail* para contato.

As provas podem ser enviadas ao *e-mail* crimedigital@mp.mg.gov.br, com a informação do número fornecido pelo sistema da Promotoria Estadual de Combate aos Crimes Cibernéticos, ou por meio de um complemento da denúncia, efetuado no sistema da Promotoria, anexando os arquivos.



São exemplos de infrações penais de ação pública condicionada:

- **Ameaça** (art. 147 do Código Penal);
- **Corrupção de menores** (art. 218 do Código Penal);
- **Crime contra a honra de funcionário público, cometido em razão de suas funções** (art. 141, II, c/c art. 145, parágrafo único, do Código de Processo Penal);
- **Violação de comunicação telegráfica, radioelétrica ou telefônica** (art. 151 do Código Penal).



4.3 - Ação penal privada

Ação penal privada é aquela em que o direito de promover a ação penal pertence ao ofendido ou a quem tenha qualidade para representá-lo.

São exemplos de infrações penais de ação privada:

- **Injúria** (art. 140 do Código Penal);
- **Calúnia** (art. 138 do Código Penal);
- **Difamação** (art. 139 do Código Penal);
- **Dano** (art. 163 do Código Penal).

OBS.: Apesar da ação penal privada, pode o cidadão que se sentir lesado em seus direitos notificar diretamente o prestador do serviço de conteúdo para que remova o conteúdo ilegal ou ofensivo de seus servidores e preserve todas as provas de materialidade e os indícios de autoria do crime. Um modelo de carta ao provedor pode ser baixado do site da Promotoria Estadual de Combate aos Crimes Cibernéticos, na pasta “Modelos” (www.mp.mg.gov.br – Portal Crime Digital).



Calúnia, injúria, difamação são considerados crimes de ação penal privada. Nesses casos, o Ministério Público não tem legitimidade para promover a ação penal. Por isso, caberá ao ofendido, ou ao seu representante legal, a propositura da ação penal, por meio de advogado. Se a pessoa ofendida não tiver informações e provas suficientes para a propositura da ação, pode procurar a delegacia especializada para requerer a instauração de inquérito policial.

Os endereços das delegacias especializadas estão disponíveis em **www.mp.mg.gov.br** - Clicar em Crimes Cibernéticos.



5. Referências

BLOG. Disponível em: <http://pt.wikipedia.org/wiki/Blog>. Acesso em: 12 Dez 2011.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANÇA. Disponível em: <http://www.mnp.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.

FACEBOOK. Disponível em: <https://www.facebook.com/help/174210519303259/>. Acesso em: 23 nov. 2012.

FACEBOOK. Disponível em: <https://www.facebook.com/help/187721894638019>. Acesso em: 23 nov. 2012.

FACEBOOK. Disponível em: <https://www.facebook.com/legal/proposeddup/pt>. Acesso em: 23 nov. 2012.

G1. Homem é preso em MG por suspeita de estelionato em site de leilões. Disponível em: <http://g1.globo.com/minas-gerais/noticia/2012/06/homem-e-preso-em-mg-por-suspeita-de-estelionato-em-site-de-leiloes.html>. Acesso em: 23 nov. 2012.

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+TWTTER.html>. Acesso em: 12 dez. 2011.

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

GREGO, Maurício. Facebook cresceu 54% no Brasil em seis meses. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/facebook-cresceu-54-no-brasil-em-seis-meses/>. Acesso em: 23 nov. 2012.

MACACOBOBO. Vírus brasileiro se espalha por chat. Disponível em: <http://macacobobo.blogspot.com.br/2011/06/virus-brasileiro-se-espalha-por-chat-do.html>. Acesso em: 7 dez. 2012.

MICROSOFT. Windows Live Proteção para a Família. Disponível em: <http://go.microsoft.com/fwlink/?LinkID=255475>. Acesso em: 10 dez. 2012.

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

MOVIMENTO CRIANÇA MAIS SEGURA NA INTERNET. Guia de postura em redes sociais. Disponível em: http://www.criancamaissegura.com.br/cartilha_guiaredessociais.pdf. Acesso em: 12 dez 2011.

Movimento Internet Segura. Disponível em: <http://www.internetsegura.org>. Acesso em: 30 set. 2008.

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



NUCCI, Guilherme de Souza. *Manual de Processo Penal e Execução Penal*. 2ª ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2006.

Núcleo de Informação e Coordenação do Ponto br. Disponível em: <<http://cartilha.cert.br>>. Acesso em: 30 set. 2008.

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

PACHECO, Denílson Feitoza. *Direito Processual Penal. Teoria, Crítica e Práxis*. 3ª ed. rev. ampl. e atual. com Emenda Constitucional da "Reforma do Judiciário". Niterói, RJ: Impetus, 2005. 1400 p.

PcWorld. Now! Digital Business. Disponível em: <<http://pcworld.uol.com.br/dicas/2008/10/09/proteja-seus-filhos-monitorando-e-limitando-o-que-eles-fazem-no-pc>>. Acesso em: 30 set. 2008.

RAMOS JUNIOR, Hélio Santiago. *Estudo sobre a Aplicabilidade das Leis Penais aos Crimes Informáticos no Brasil*. The Third International Conference of Forensic Computer Science. ISSN 1980-1114. v. 3. N.1. 2008.

RECLAME AQUI, o Maior Site da América Latina em Defesa do Consumidor. Disponível em: <<http://www.reclameaqui.com.br>>. Acesso em: 16 jul. 2009.

Safernet Brasil. Disponível em: <<http://www.safernet.org.br/wiki/bin/view/SaferNet/OutrosCrimes>> Acesso em: 15 set. 2008.

SEMPRETOPS. Usuários de Xbox em perigo. Disponível em: <http://www.sempretops.com/games/usuarios-de-xbox-em-perigo/>. Acesso em: 07 Dez. 2012.

SUPERIOR TRIBUNAL DE JUSTIÇA. Conflito de competência n.º 112.616 - PR (2010/0107983-8). Disponível em: <<http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=%28%22GILSON+DIPP%22%29.min.&data=%40DTDE+%3E%3D+20110413+e+%40DTDE+%3C%3D+20110413&&b=ACOR&p=true&t=&l=10&i=2>>. Acesso em: 30 nov. 2011.

TWITTER, Ivete Sangalo. Disponível em: <<https://twitter.com/ivetesangalo>>. Acesso em: 7 dez. 2012.

TWITTER. Disponível em: <http://pt.wikipedia.org/wiki/Twitter>. Acesso em: 12 Dez. 2011.

TWITTER. Termos e Condições de Utilização dos Serviços. Disponível em: <<https://twitter.com/tos>>. Acesso em: 10 dez. 2012.

WIKIPEDIA. Verbetes on-line Disponível em: <http://pt.wikipedia.org/wiki/Jogo_on-line>. Acesso em: 23 nov. 2012.

XBOX 360. Disponível em: <<http://www.xbox.com/pt-BR/Xbox360/Consoles/Home-new?xr=shellnav>>. Acesso em: 7 dez. 2012.



www.mp.mg.gov.br

crimedigital@mp.mg.gov.br

(31) 3330 8401





Navegar com
Segurança